U.S. Army War College
Dept. of Military Strategy, Planning, and Operations

January 2006
AY06 Edition

U.S. Army War College

Information Operations Primer

Fundamentals of Information Operations

DEPARTMENT OF THE ARMY
UNITED STATES ARMY WAR COLLEGE AND CARLISLE BARRACKS
CARLISLE, PENNSYLVANIA 17013-5217

REPLY TO
ATTENTION OF

ATWC-A 11 January 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Information Operations Primer

This is a document prepared primarily for use by the staff, faculty, and students of the U.S. Army War College. It is not intended for general distribution and may not be copied or otherwise distributed as a whole without specific permission from the Commandant, U.S. Army War College, in each instance.

William T. Johnsen
WILLIAM T. JOHNSEN, Ph.D.
Dean of Academics

DISTRIBUTION:
DMSPO 550

This Page Intentionally Blank

Return to Contents

Forward

This document provides an overview of Department of Defense (DOD) Information Operations (IO) doctrine and organizations at the joint and individual service levels. It is intended to serve students and staff of the US Army War College as a ready reference for IO information extracted and summarized from a variety of sources. Wherever possible, Internet web sites have been given to provide access to additional and more up-to-date information. The booklet is intentionally UNCLASSIFIED so that the material can be easily referenced during course work, while engaged in exercises, and later in subsequent assignments.

This booklet begins with an overview of Information Operations. It then examines the critical concept of information superiority presented in *Joint Vision 2020*. Current IO doctrine at the joint and service levels are then summarized. Relevant organizations dedicated to IO are identified along with their respective missions and capabilities. Finally, the document concludes with an overview of Information Operations Conditions (INFOCONS) and an IO specific glossary.

Readers will note that many of the concepts, documents, and organizations are "works in progress" as DoD and the services strive to address the challenges of a rapidly changing IO environment. Thus, this summarization effort is on-going and continuous. Please address any suggested additions, revisions and/or corrections to the primary point of contact below for inclusion in subsequent editions.

Special thanks and recognition is given to the Information Warfare Group, USAWC Center for Strategic Leadership, and to the following individuals throughout the Department of Defense whose help and assistance have made this revision of the Primer possible: Ms. Chris Adams (Joint Warfare Analysis Center, Dahlgren, VA), Maj Marc Alexander, USMC (Marine Corps Combat Development Command); COL Mike Carroll, USA (Joint Staff DDGO); LTC John Cox, USA (JTF-GNO); SSgt Aaron Cram USAF (USSTRATCOM); Mr. Donald Jones (OASD-NII); Maj Scott Langan, USAF (Air Force Information Warfare Center); Mr. William D. Malone (Navy Information Operations Command); LTC James 'Bo' Merchant, USA (USSOCOM); LtCol Robert Morris, USAF (OUSD-I); Col Richard Rayfield, USMC, Mr. Ric Coronado and Mr. Anthony Maybrier (all of JIOC); Ms. Tara Shea (IATAC); Mr. Mike Strain (DPO-MA); Mr. Steve Shires and Mr. Eric Vernon (1st IO Cmd); and LTC Steven Whitmarsh, USA (OUSD-P).

COL David J. Smith
Department of Military Strategy, Planning, and Operations
U.S. Army War College
Carlisle, PA 17013-5242
(717) 245-3455
david.smith@carlisle.army.mil

Return to Contents

This Page Intentionally Blank

Return to Contents

TABLE OF CONTENTS

Return to Contents

Introduction

Introduction to Information Operations

Few topics seem to have as much controversy or discussion as, "What constitutes Information Operations (IO)?" This introduction attempts to answer that question by examining IO both conceptually and doctrinally. It is intended as a guide to the topic to facilitate academic discussion and is not authoritative. Throughout this discussion, various terms will be defined informally to facilitate understanding and comprehension. The reader is directed to Joint Publication 1-02, as required, for the approved formal definitions. Note: DoDD 3600.1 and the revised JP 3-13 have more current definitions of several key terms which are not yet reflected in JP 1-02.

Information Operations is an evolving construct with historical roots back to antiquity. Thus it is both an old and a new concept. The late 1970's saw the emergence of Information Warfare (IW) as a war-fighting construct by integrating several diverse capabilities. IW, in turn, evolved into Information Operations recognizing the critical role of information as an element of national power through the full spectrum of peace, conflict, and war.

So what is Information Operations?

1. <u>**IO as an Integrating Function.**</u> **Information Operations is essentially the *integration* of specified activities involving information and information systems.** This concept is similar to Joint Operations which is the integration of service capabilities or Combined Operations which is the integration of battlefield operating system capabilities. The integration envisioned as not mere deconfliction, but the synchronization and harmonization of activities whose resulting effect is significantly greater than the sum of the individual components. While this writes well and briefs well, it is the foundation for successful employment of IO.

IO is normally performed by military forces at both the operational and tactical levels. IO at the strategic level is a critical component of strategic communication.

Several questions logically follow:

a. What activities are integrated?

b. How are they integrated?

c. Towards what end?

Following the concept of "begin with the end in mind," the last question will be considered first.

2. <u>**Purpose of IO – Offensive.**</u> **Information Operations seeks to influence the *behavior* of target decision-makers or audiences through the use of information and information systems.** This is no different from the exercise of the other forms of national power, be they diplomatic, military, or economic. In this instance the means is information, but the resulting outcome is the same.

a This use of information is frequently referred to as "soft-power" or "non-kinetic" as contrasted with the military use of kinetic (both lethal and nonlethal) means to physically attack a target.

b. However, IO also encompasses activities to disrupt, degrade, or destroy target adversary information systems. This includes physical destruction. Isolating an enemy decision-maker by eliminating his ability to command and control his forces is certainly a means of influencing his behavior.

c. Note the use of the term "target" vice "adversary" or "enemy." IO can be used to influence a wide range of potential audiences. Fortunately, the use of IO to influence domestic audiences is strictly prohibited to prevent abuse of this capability.

d. Often times affecting the target's decision cycle (sometimes referred to as his "OODA-loop" (observe, orient, decide, act - loop)) is a means of influencing target behavior. Obviously, reducing an adversary's ability to make timely and effective decisions will degrade his exercise of initiative or his response to friendly military action.

e. Actions taken to influence target behavior are normally categorized as offensive.

3. **<u>Purpose of IO – Defensive.</u> Information Operations also seeks to shield or defend friendly decision-makers or audiences from being unduly influenced by a target's use of information or information systems.**

a. In this instance, the target is more likely to be on the "adversary" or "enemy" end of the spectrum.

b. These shielding or defending actions are not intended to prevent the unrestricted flow of information vital to a free society. They are intended to prevent a target's manipulation or distortion of information from being effective.

c. Also included are actions to protect friendly information and information systems from compromise or disruption. These systems are seen as vital to ensure friendly ability to maintain situational awareness and to command/control their forces.

d. Actions taken to limit a target's ability to influence friendly behavior are categorized as defensive.

4. **<u>An IO Conceptual Model.</u>** At this point, a model would be helpful to conceptualize the kind of activities which would be effective in achieving the desired result (influence target behavior, protect friendly behavior from being influenced).

a. All Information Operations activities occur within the broader context of an ***information environment***. This environment recognizes the critical role that information and information systems play in today's advanced societies as they progressed along a continuum from agrarian, to industrial, to the information age. This environment pervades and transcends the boundaries of land, sea, air, and space.

b. Within this environment exists three conceptual domains: physical, information, and cognitive as depicted in Figure 1, representing a target's decision cycle.

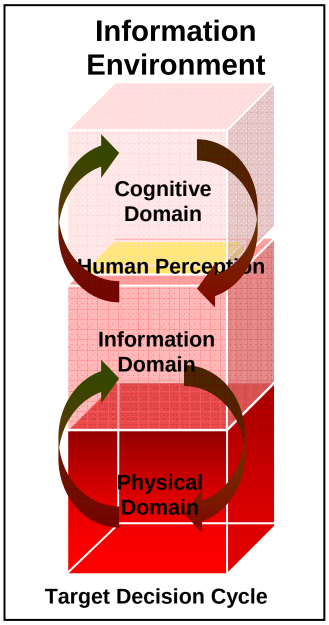


Figure 1. Information Environment

(1) The physical domain is the tangible real word. It is the domain where military operations take place within the land, sea, air, and space environments. Information systems and communications systems (infra-

structure) exist within this domain to enable these operations to take place

(2) The information domain is where information is created, manipulated, shared, and stored. This domain links the physical real world with the human consciousness of the cognitive domain both as a source of input (stimulus, senses, etc.) and to convey output (intent, direction, decisions, etc.). These linkages are shown as arrows in the figure.

(3) The cognitive domain exists in the mind. Here is where the individual processes the received information according to a unique set of norms, morals, beliefs, culture, and values. These attributes act as a human perception "window" to filter the information and provide a sense of meaning and context. The information is evaluated and processed (via an O-O-D-A loop or other model) to form decisions which are communicated back through the information domain to the physical world. It should be noted that the cognitive domain can not be directly attacked (short of mind-altering drugs, etc.) but must be influenced indirectly through the physical and information domains.

(4) Not shown in the figure is an additional "social" domain which links the individual to others forming a greater social network. This social network plays a critical role in the human decision-making process as well.

c. In a similar manner, the friendly decision cycle can be represented in relationship to the target as shown in Figure 2. This allows several terms to be defined conceptually.

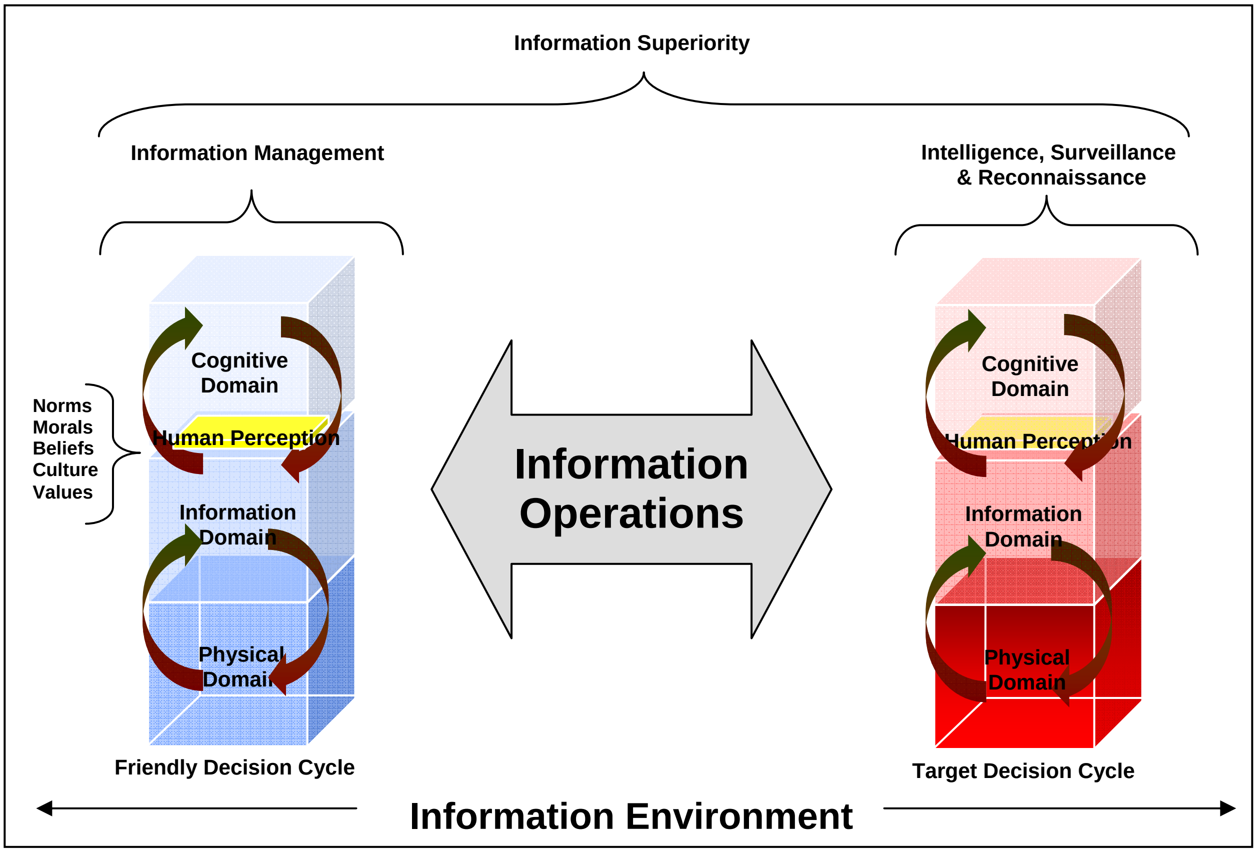


Figure 2. A Notional Information Operations Model

(1) **Intelligence, Surveillance, and Reconnaissance (ISR)** are those activities which synchronize and integrate the planning and operation of sensors, assets, and processing, exploitation, and

Return to Contents

dissemination systems to gain information and knowledge concerning a target (adversary). The focus is strictly on target information and information systems.

(2) Correspondingly, **Information Management (IM)** activities seek to provide the right information to the right individual at the right time in a usable form to facilitate situational understanding and decision-making. The focus is on friendly information and information systems.

(3) The third type of activity relates to both friendly and target decision cycles. These activities, either offensive or defensive in nature, are **Information Operations (IO)** as indicated in Figure 2.

(4) Considering these three sets of activities as a whole yields **Information Superiority** which, when achieved, results in a degree of dominance in the information domain (environment) permitting the conduct of operations without effective opposition. Information Superiority is a key enabler of Joint Vision 2020 and Network-centric Operations.

d. Applying the previous categorization of IO activities as either offensive or defensive to the model provides an additional level of understanding as shown in Figure 3.

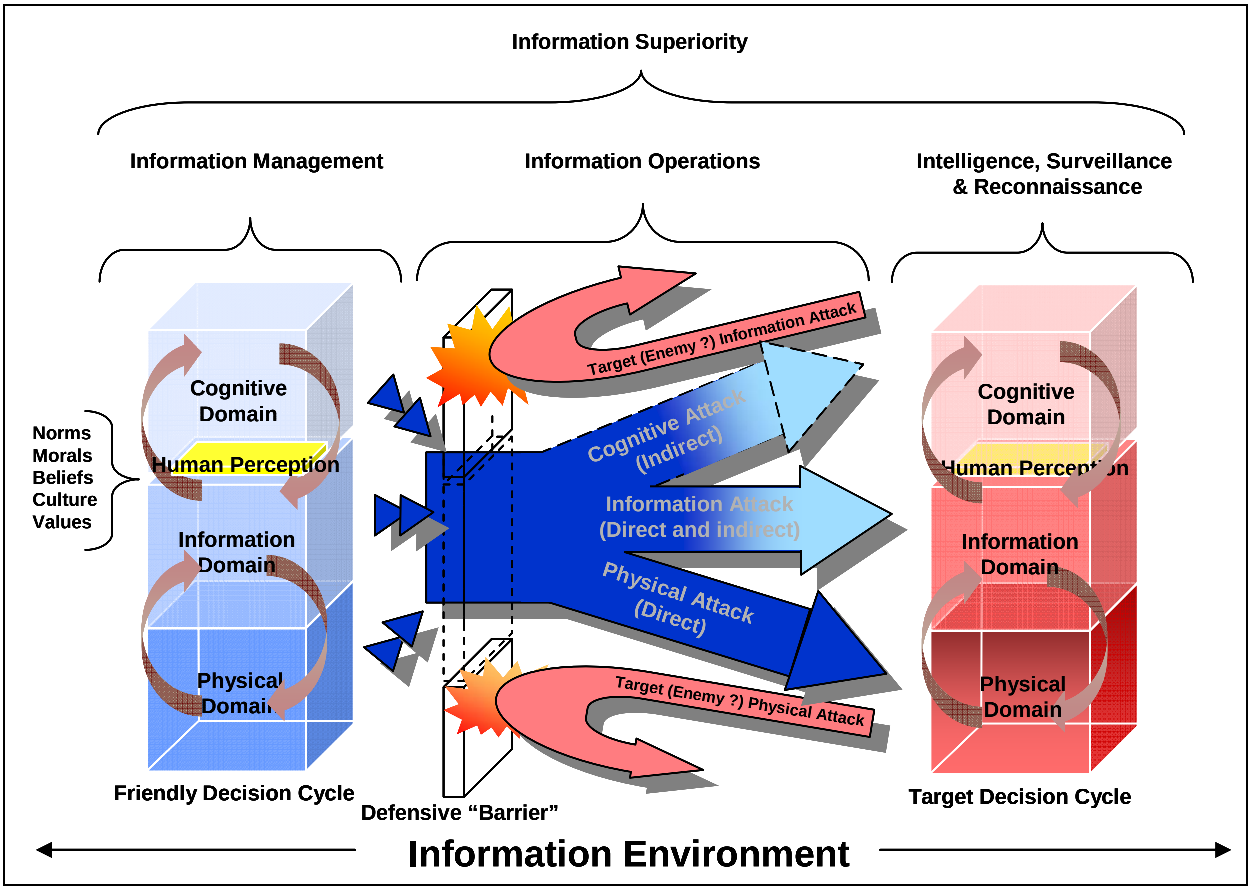


Figure 3. Information Operations Conceptual Framework

(1) Offensive IO actions are shown directed against target (adversary/enemy) physical, information, and cognitive (indirectly) domains.

(2) Defensive IO actions are shown as a barrier (wall) shielding the friendly decision cycle from target (adversary/enemy) attacks.

5. **IO Activities.** Using this framework, it is now possible to address the question of what activities are integrated by IO. These activities will be further categorized as either core, supporting, or related capabilities.

a. Core capabilities are those which are essential to the conduct of IO by providing critical operational effects or preventing the adversary from doing so. The five core capabilities of Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO) form the foundation for IO. While not every activity conducted within these capabilities is IO, they all contribute to the achievement of IO objectives.

(1) **Psychological Operations (PSYOP)** are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, and individuals. The purpose of PSYOP is to induce or reinforce attitudes and behavior favorable to friendly objectives.

(2) **Military Deception (MILDEC)** is those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Note: MILDEC and OPSEC are complementary activities. MILDEC seeks to encourage incorrect adversary analysis so as to arrive at a specific false conclusion. OPSEC seeks to obscure or deny real information to an adversary preventing him from correctly deducing friendly plans and intentions.

(3) **Operations Security (OPSEC)** is a process of identifying critical information and subsequently analyzing friendly actions and other activities to: identify what friendly information is necessary for an adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remains secure.

(4) **Electronic Warfare (EW)** is any military action involving the use of the electromagnetic (EM) spectrum and directed energy to control the EM spectrum or to attack the adversary. EW is further categorized into three major subdivisions:

(a) Electronic Attack (EA) is the use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability.

(b) Electronic Protection (EP) ensures the friendly use of the electromagnetic spectrum.

(c) Electronic Warfare Support (ES) is actions taken to search for, intercept, identify, locate, or localize sources of intentional or unintentional radiated EM energy for subsequent action.

(5) **Computer Network Operations (CNO)** is any operation employing computer networks to attack, exploit, or defend electronic information in computer networks and the supporting computer network infrastructure. Like Electronic Warfare, it may be further categorized into three subdivisions:

(a) Computer Network Attack (CNA) consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers, and computer networks, or the computers and networks themselves.

(b) Computer Network Defense (CND) are actions taken through the use of computer networks to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

Return to Contents

(c) Computer Network Exploitation (CNE) are enabling operations and intelligence collection conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

b. These five core capabilities are supported by five additional capabilities which provide additional, though less critical, operational effects. Counterintelligence (CI), Combat Camera (COMCAM), Physical Attack, Physical Security, and Information Assurance (IA)

(1) **Counterintelligence (CI)** consists of information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(2) **Combat Camera (COMCAM)** consists of visual information documentation covering air, sea, and ground actions of the Armed Forces of the United States in combat or combat support operations and in related peacetime training activities such as exercises, war games and operations.

(3) **Physical Attack** are actions taken to employ of kinetic fires (to include kinetic, nonlethal fires) against physical information targets.

(4) **Physical Security** are measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft.

(5) **Information Assurance (IA)** are measures that protect and defend electronic information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

c. Finally, three additional related capabilities of Pubic Affairs (PA), Civil-Military Operations (CMO), and Defense Support to Public Diplomacy (DSPD) contribute to the accomplishment of the IO mission. These activities often have regulatory, statutory, or policy restrictions and limitations regarding their employment which must be observed.

(1) **Public Affairs (PA)** are those public information, command information, and community relations activities directed towards both the external and internal publics with interest in the Department of Defense.

(2) **Civil-Military Operations (CMO)** are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives.

(3) **Defense Support to Public Diplomacy (DSPD)** are those activities and measures taken by DoD components, non solely in the area of IO, to support and facilitate overt public diplomacy efforts of the USG and its departments and agencies (previously called Military Support to Public Diplomacy).

Return to Contents

d. These capabilities can be summarized as shown in the following table.

<table>
<tr><th colspan="2"><u>CORE CAPABILITIES</u></th></tr>
<tr><td>Electronic Warfare
Computer Network Operations
Operations Security</td><td>Military Deception
Psychological Operations</td></tr>
<tr><th><u>SUPPORTING CAPABILITIES</u></th><th><u>RELATED CAPABILITIES</u></th></tr>
<tr><td>Information Assurance
Physical Security
Counterintelligence
Physical Attack
Combat Camera</td><td>Public Affairs
Civil-Military Operations
Defense Support to Public Diplomacy</td></tr>
<tr><td colspan="2"><b><u>DoD Information Operations:</u></b> “The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own.”</td></tr>
</table>

Table 1. Joint IO Definition

e. These activities can be related to the IO Conceptual Framework previously described in terms of offensive and defensive actions as well as in terms of their orientation with respect to the cognitive, information, and physical domains. An additional distinction which may be helpful is to further categorize the activities into those which are primarily “influential” in nature (MILDEP, PSYOP, PA, etc.) and those which are more “technical (or electronic)” in nature (EW and CNO, etc.). Note: The revised JP 3-13 has dropped the distinction between offensive and defensive operations. Likewise, DoD does not concur with the segregation of these activities into “influence” and “technical” operations. However, the author has found that some distinctions are helpful “conceptually” while still appreciating the fact that the real power of IO comes from their integrated application.

6. **IO Planning and Execution.** Having identified the purpose of IO and the activities associated with it, the third question will now be addressed concerning how IO activities (capabilities) are integrated.

a. Information Operations are planned by the IO section of a joint or service staff under the direction and supervision of a designed IO officer. Normally this section resides within the operations division (J-3) of the staff. Current Army IO doctrine designated the creation of a separate primary staff section (G-7) responsible for IO planning and execution.

b. To further integrate and synchronize IO activities, an “IO Cell” is established under the leadership of the IO officer. Representatives from the core, supporting, and related activities as well as the special staff, service/functional components, and appropriate national agencies serve as members.

c. IO planning should be fully integrated into the overall joint planning process, be it contingency or crisis action. There should not be a separate “IO campaign plan” just there is not a separate “maneuver campaign plan.”

d. Products from the IO planning process are incorporated into the Commander’s Estimate, Commander’s Concept, and the OPLAN/OPORD as documented in Joint Operation Planning and Execution System (JOPES).

e. Additionally, IO planners and operators must be represented within the Effects and Effects Coordination Cell where operational fires (both kinetic and non-kinetic) are integrated and synchronized.

f. Execution of the IO portion of the joint plan is done by both dedicated IO forces (PSYOP, EW, CNO, etc.) and general purpose forces tasked for that purpose (MILDEP, OPSEC, etc.).

g. Evaluation of the success of the execution of the plan is done through identified measures of effectiveness (how well the plan achieved the desired result) as well as through measures of performance (how well the plan was executed).

7. **Additional Considerations.**

a. IO effects typically take longer to achieve and are more difficult to measure than conventional operations. Therefore, a long term commitment to effectively employ information to affect target behavior is critical. Theater Security Cooperation Plans are a vital part of this effort. Waiting until a crisis occurs and then “throwing info ops at it” is an exercise in futility. Likewise, the idea of employing decisive combat operations in one area while employing information operations in other as a kind of economy of force measure is a misapplication of IO.

b. An appropriate understanding of the target’s culture and norms is also critical. The tendency to “mirror” friendly cultural values and perspectives must be avoided at all costs. The preparation of IO products and an evaluation of their potential effectiveness must be done from the perspective of the recipient (target audience) through their cultural lens. This is especially true during the “product review and approval” process when what may appear to be an unsophisticated and even amateurish looking product (leaflet, flyer, handbill, etc.) may, in fact, be exactly the proper vehicle for conveying the desired message.

Effective IO leverages the power of information to compliment the other instruments of national power resulting in the achievement of national objectives with less expenditure of blood and treasure.

COL David J. Smith
Department of Military Strategy, Planning, and Operations
U.S. Army War College

Updated: January 2006.

Return to Contents

Strategic Communication

This section addresses some considerations of the information element of power at the strategic level.

a. Information and National Power. Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents allude to different aspects of information but without a specific strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power…and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: “use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security.”[3] Information as power is wielded in an increasingly complex environment consisting of the physical, information, and cognitive domain as previously defined.

b. The executive branch of the US government has the responsibility to develop and sustain an information strategy that ensures that consistent policy, themes, and messages are promulgated. This strategy should guide and direct communications activities across the information environment. (Given the “ends, ways, means” model these activities constitute the “ways”). Effective Strategic Communication is the desired “end” within that strategy. **Strategic Communication** can be described as the proactive and continuous process that supports the national security strategy by identifying and responding to strategic threats and opportunities with information related activities. It is the transmission of integrated and coordinated USG themes and messages that advance US interests and policies though a synchronized interagency effort supported by public diplomacy (PD), public affairs (PA), and related elements of IO, in concert with other political, economic, information, and military actions.[4]

(1) Public affairs and military IO have been defined in the context of their use within the Department of Defense (DOD) in the previous section.

[1] Reagan, Ronald. National Security Decision Directive 130. Washington, D.C.: The White House, 6 March 1984. Available from http://www.fas.org/irp/offdocs/nsdd/nsdd -130.htm. Internet. Accessed 23 December 2005.

[2] Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as “Instruments of Power.” It further states that Information, while not an instrument of power, forms a backdrop as all activity has an informational backdrop.

[3] Neilson, Robert E. and Daniel T. Kuehl, “Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program. National Security Strategy Quarterly (Autumn 1999): 40.

[4] Various definitions of strategic communication exist. The one shown here is taken from U.S. Department of Defense. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington, D.C.: U.S. Department of Defense, final coordinating draft dated 5 July 2005.

(2) Public diplomacy is primarily practiced by the Department of State (DOS). It is defined as those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. Public diplomacy is traditionally focused on foreign elite: person to person contacts with press, business leaders, officials, other opinion leaders.

(3) International broadcasting services are cited as a strategic communication means in some definitions. Under the supervision of the Broadcasting Board of Governors (BBG), the International Broadcasting Bureau (IBB) provides the administrative and engineering support for U.S. government-funded non-military international broadcast services. Broadcast elements are the Voice of America (VOA) and Radio and TV Martí (Office of Cuba Broadcasting). In addition, the IBB provides engineering and program support to Radio Free Europe/Radio Liberty, Radio Free Asia, the Middle East Broadcasting Networks (Radio Sawa and Alhurra Television), and Radio Farda, a joint Persian-language project between VOA and Radio Free Europe.[5]

Strategic communication has generally been considered a national strategic concept, however, it is increasingly addressed at the theater strategic level as well.

c. History of Strategic Communication. While “strategic communication” is a fairly new term in the U.S. government lexicon, the concept, theory, and practice behind it is not. Winfield Scott recognized the importance of strategic communication at the theater level in Veracruz in 1847. Realizing the influence of the Catholic Church on Mexican society, Scott attended Mass with his staff at the Veracruz Cathedral to display the respect of U.S. forces. He further ordered U.S. soldiers to salute Mexican priests in the streets. Each of these measures was “part of a calculated campaign to win the friendship of the Mexicans.”[6]

The recent history of national strategic communication shows concerted efforts to positively portray the U.S. story in order to persuade and influence.

(1) The Committee on Public Information (1917), also known as the Creel Committee after its chief newspaperman George Creel, sought to rally U.S. public opinion behind World War I on behalf of the Wilson administration. Its focus was the domestic audience and it used public speakers, advertising, pamphlets, periodicals, and the burgeoning American motion picture industry.

(2) The Office of War Information (1942) focused both domestically and overseas, with broadcasts sent in German to Nazi Germany. The Voice of America (VOA) began its first broadcast with the statement, "Here speaks a voice from America. Everyday at this time we will bring you the news of the war. The news may be good. The news may be bad. We shall tell you the truth”.

(3) The Smith-Mundt Act (1948) (actually, “The U.S. Information and Educational Exchange Act (Public Law 402; 80th Congress)”), established a statutory information agency for the first time in a period of peace with a mission to "promote a better understanding of the United States in other countries,

[5] The United States Government’s International Broadcasting Bureau. Available from: http://www.ibb.gov. Internet. Accessed 23 December 2005.

[6] Eisenhower, John S.D. *Agent of Destiny: The Life and Times of General Winfield Scott*. New York: The Free Press, 1997, 245-6.

and to increase mutual understanding" between Americans and foreigners. The act also forbade the Voice of America to transmit to an American audience.[7]

(4) The United States Information Agency (USIA) (1953) was established by President Eisenhower as authorized by the Smith-Mundt Act. It encompassed all the information programs, including VOA (its largest element), that were previously in the Department of State, except for the educational exchange programs, which remained at State. The USIA Director reported to the President through the National Security Council and received complete, day-to-day guidance on U.S. foreign policy from the Secretary of State.

(5) A 1998 State Department reorganization occurred in response to calls by some to reduce the size of the U.S. foreign affairs establishment. (This is considered the State Department's "peace dividend" following the Cold War). The act folded the USIA into the Department of State. It pulled the Broadcasting Board of Governors out of USIA and made it a separate organization. The USIA slots were distributed throughout the State Department and its mission was given to the Bureau of International Information Programs.

d. National Strategic Communication: Current Models and Processes. The demise of USIA is generally regarded (in retrospect) as diluting the ability of the United States to effectively promulgate a national communication strategy, coordinate and integrate strategic themes and messages and support public diplomacy efforts worldwide.[8] Additionally organizations and processes have experienced great flux in recent years. The current administration retained Presidential Decision Directive (PDD) 68 that was enacted in 1999 by the Clinton administration. PDD 68 addressed those problems when no single U.S. agency was empowered to coordinate US efforts to sell its policies and counteract bad press abroad. It directed top officials from the Defense, State, Justice, Commerce and Treasury departments as well as those from the Central Intelligence Agency and FBI to establish an International Public Information (IPI) Core Group chaired by the Under Secretary for Public Diplomacy and Public Affairs at the Department of State.[9] It is evident, however that this core group is currently inactive. Other recent initiatives to coordinate and integrate national strategic communication efforts have also faltered. The White House Office of Global Communication was disbanded in 2003. A Strategic Communication Policy Coordinating Committee (PCC) met on several occasions, but is currently inactive. A Muslim Outreach Policy Coordinating Committee is more active and in fact, developed a draft national communication strategy that has yet to be adopted.[10] A recent proposed reorganization of the National Security Council to include a Deputy National Security Advisor for Strategic Communication remains dormant. On the other hand, an Interagency Strategic Communication Fusion Team is an active, albeit informal, coordinating body at the action officer level. Team members share information about their respective plans and activities in order to leverage each other's communication with international publics. The team coordinates and de-conflicts the production and the dissemination of information products but does not

[7] The Smith-Mundt Act is still in effect to include the requirement not to "target" U.S. audiences. The current information environment with ubiquitous, world-wide media outlets, satellite communications and real-time reporting makes it difficult to target foreign audiences without exposing U.S. audiences to the message, however…a fact not envisioned in 1948 when the act became effective and one that continues to cause friction between the military and media.

[8] Kaplan, David E. "Hearts, Minds, and Dollars." *U.S. News and World Report*, 25 April 05, 25, 27.

[9] Federation of American Scientists. Intelligence Resource Program. *U.S. International Public Information (IPI).* Presidential Decision Directive PDD 68, 30 April 1999. Available from http:// www.fas.org/irp/offdocs /pdd/pdd-68.htm. Internet. Accessed 23 December 2005.

[10] U.S. General Accounting Office. *U.S. Public Diplomacy*. Washington, D.C.: U.S. General Accounting Office, April 2005. 10-13.

task. Instead, team members reach across office, bureau and agency boundaries to offer or to seek support for their strategic communication plans and activities.[11]

Ambassador Karen Hughes assumed duties as the Under Secretary of State for Public Diplomacy and Public Affairs in the early fall of 2005. The Under Secretary helps ensure that public diplomacy (engaging, informing, and influencing key international audiences) is practiced in harmony with public affairs (outreach to Americans) and traditional diplomacy to advance U.S. interests and security and to provide the moral basis for U.S. leadership in the world.[12] As of this writing it has yet to be determined if Ambassador Hughes' efforts will result in development of a formal communication strategy, along with enduring strategic communication processes, capacity, resources and organizational structures to promulgate that strategy.

e. Theater Strategic Communication. Theater strategic communication is an emergent concept with only brief discussion in Joint Publication 3-13 (final coordinating draft). However, because of the capacity gaps at the national level (as described above), and the importance of the information element of power in the current Global War on Terrorism (GWOT), most Combatant Commanders have established processes and organizations to address the need. An unclassified draft annex on strategic communication in the National Military Strategic Plan for the War on Terrorism[13] directs Combatant Commanders to develop internal processes and, where appropriate, organizations for integrating strategic communication within Combatant Command plans and operations. This annex further indicates that Combatant Commanders, when appropriate, may identify a strategic communication director. The principal responsibility of this position is to communicate and plan communications. CENTCOM has established a robust strategic communication directorate; other combatant commands have not, but instead have used other models for this purpose. While national strategic communication consists of PA, PD and IO, theater strategic communication includes military PA, defense support to public diplomacy (alternately referred to as military support to public diplomacy), and IO. The concept of defense support to public diplomacy is still vaguely defined with examples ranging from theater web initiatives aimed at certain regions and demographics within those regions to theater logistical support to embassies and diplomatic staffs. Beyond the importance of theater strategic communications in the current phase of the GWOT, emergent doctrine is correct to point out the importance of strategic communication activities in implementing theater security cooperation plans (TSCPs).[14]

Professor Dennis Murphy
Information Warfare Group
Center for Strategic Leadership
U.S. Army War College

Updated: January 2006

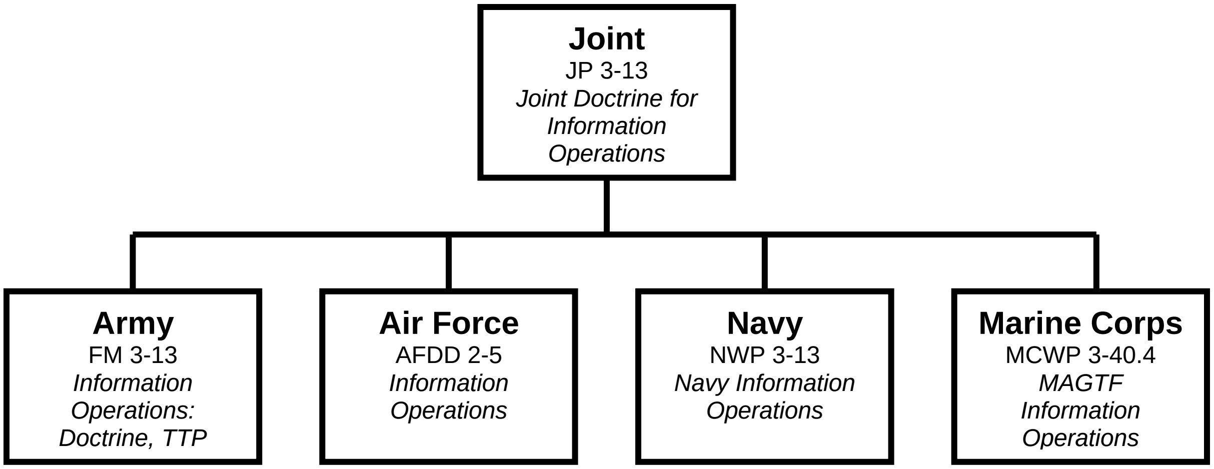
[11] Interagency Strategic Communication Fusion Team. Meeting summary, 16 December 2005: 3.

[12] U.S. Department of State. Senior Officials: Under Secretary for Public Diplomacy and Public Affairs -- Karen Hughes. Available from http://www.state.gov/misc/19232.htm. Internet. Accessed 23 December 2005.

[13] U.S. Department of Defense. *National Military Strategic Plan for the War on Terrorism, Strategic Communication (DRAFT): Annex H*. Washington, D.C.: U.S. Department of Defense, 18 April 2005.

[14] Joint Publication 3-13, I-13.

Joint and Service Doctrine



Joint
JP 3-13
Joint Doctrine for Information Operations

Army
FM 3-13
Information Operations: Doctrine, TTP

Air Force
AFDD 2-5
Information Operations

Navy
NWP 3-13
Navy Information Operations

Marine Corps
MCWP 3-40.4
MAGTF Information Operations

This Page Intentionally Blank

Return to Contents

Joint Vision 2020 and Information Superiority

Complete JV2020 (Jun 2000) is available at: http://www.dtic.mil/jointvision/jvpub2.htm

Key elements of the Vision related to Information Operations

- **Threat.** "In 2020, the nation will face a wide range of interests, opportunities, and challenges and will require a military that can both win wars and contribute to peace. The global interests and responsibilities of the United States will endure, and there is no indication that threats to those interests and responsibilities, or to our allies, will disappear. The strategic concepts of decisive force, power projection, overseas presence, and strategic agility will continue to govern our efforts to fulfill those responsibilities and meet the challenges of the future."

  "…potential adversaries will have access to the global commercial industrial base and much of the same technology as the U.S. military. We will not necessarily sustain a wide technological advantage over our adversaries in all areas. Increased availability of commercial satellites, digital communications, and the public internet all give adversaries new capabilities at a relatively low cost."

- **Technology Drives the Four Operational Concepts.** "If our Armed Forces are to be faster, more lethal, and more precise in 2020 than they are today, we must continue to invest in and develop new military capabilities. This vision describes the ongoing transformation to those new capabilities. As first explained in *JV 2010*, and dependent upon realizing the potential of the information revolution, today's capabilities for maneuver, strike, logistics, and protection will become dominant maneuver, precision engagement, focused logistics, and full dimensional protection."

  "The overarching focus of this vision is full spectrum dominance – achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. Attaining that goal requires the steady infusion of new technology and modernization and replacement of equipment. However, material superiority alone is not sufficient. Of greater importance is the development of doctrine, organizations, training and education, leaders, and people that effectively take advantage of the technology."

- **Information Superiority is the Key Enabler.** "The evolution of these elements over the next two decades will be strongly influenced by two factors. First, the continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control."

  "The transformation of the joint force to reach full spectrum dominance rests upon information superiority as a key enabler and our capacity for innovation."

Terms/Definitions

- **Information Superiority.** "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (*Old* JP 1-02) Information superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives."

  Note: Revised JP 1-02 (5 Sep 2003) defines information superiority as "that degree of dominance in the information domain which permits the conduct of operations without effective opposition (JP 2-01.3)."

  "The word "superiority" implies a state or condition of imbalance in one's favor. Information superiority is transitory in nature and must be created and sustained by the joint force through the conduct of information operations."

- **Decision Superiority.** "Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve "decision superiority" – better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary."

  "Decision superiority results from superior information filtered through the commander's experience, knowledge, training, and judgment; the expertise of supporting staffs and other organizations; and the efficiency of associated processes."

- **Information Operations.** "…those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. (JP1-02) Information operations also include actions taken in a noncombat or ambiguous situation to protect one's own information and information systems as well as those taken to influence target information and information systems."

  "The joint force commander will conduct information operations whether facing an adversary during a conflict or engaged in humanitarian relief operations. Such operations will be synchronized with those of multinational and interagency partners as the situation dictates."

  "The commander may also employ nonkinetic weapons, particularly in the arena of information operations where the targets might be key enemy leaders or troop formations, or the opinion of an adversary population."

- **The "Grid".** "The evolution of information technology will increasingly permit us to integrate the traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. The development of a concept labeled the global information grid will provide the network-centric environment required to achieve this goal. The grid will be the globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters, policy makers, and support personnel."

Return to Contents

Challenges

- **Interoperability and Multi-National Operations.** "Technological developments that connect the information systems of partners will provide the links that lead to a common relevant operational picture and improve command and control. However, the sharing of information needed to maintain the tempo of integrated multinational operations also relies heavily on a shared understanding of operational procedures and compatible organizations. The commander must have the ability to evaluate information in its multinational context."

- **Measuring Effects of IO.** "Because the ultimate target of information operations is the human decision maker, the joint force commander will have difficulty accurately assessing the effects of those operations. This problem of "battle damage assessment" for information operations is difficult and must be explored through exercises and rigorous experimentation."

- **Understanding the Decision Process.** "Command and control is most effective when decision superiority exists. Decision superiority results from superior information filtered through the commander's experience, knowledge, training, and judgment; the expertise of supporting staffs and other organizations; and the efficiency of associated processes. While changes in the information environment have led some to focus solely on the contribution of information superiority to command and control, it is equally necessary to understand the complete realm of command and control decision making, the nature of organizational collaboration, and especially, the "human in the loop."

> ***"as new information technologies, systems, and procedures make the same detailed information available at all levels of the chain of command, leaders must understand the implications for decision-making processes, the training of decision makers at all levels, and organizational patterns and procedures."***

Conclusion

"The joint force of 2020 will use superior information and knowledge to achieve decision superiority, to support advanced command and control capabilities, and to reach the full potential of dominant maneuver, precision engagement, full dimensional protection, and focused logistics."

This Page Intentionally Blank

Return to Contents

The Information Operations (IO) Roadmap, 2003

This section provides an UNCLASSIFIED synopsis of those unclassified elements of the Road Map.

Persons who are, or will become Information Operations (IO) practitioners, should read this fundamentally important document in its entirety. The classified, 74-page, "IO Roadmap" discusses specific issues and deficiencies related to the five core IO capabilities (*PSYOP, Computer Network Operations, Military Deception, OPSEC, and Electronic Warfare*), the related DoD capabilities (Public Affairs and Civil Military Operations), and the several supporting capabilities. It addresses shortcomings in doctrine, organizational structure, and practice, it gives twelve general recommendations for improvement (see below), and it also states more than forty specific recommendations for further action.

Purpose. The Secretary of Defense, in his introduction to the Roadmap states that it seeks to advance the goal of Information Operations becoming a core military capability of U.S. forces. The current Roadmap edition (30 October 2003) aims to provide a framework for understanding Information Operations and to present a critique of the current state of IO. The Roadmap calls for a dedicated workforce, as well as development of new organizational structures that will enhance IO, and also support Defense Transformation efforts

Three IO Functional Areas. The Roadmap broadly defines three integrated functional areas that include the five IO core capabilities, as follows:

1. Those activities aimed at deterring, discouraging, dissuading, and directing an adversary, thereby disrupting his unity of command and purpose while preserving our own (PSYOP).

2. Protecting our plans while misdirecting theirs, thereby allowing our forces to mass their effects to maximum advantage while the adversary expends his resources to little effect (OPSEC and Military Deception).

3. Control adversarial communications networks while protecting ours (Electronic Warfare and Computer Network Operations).

The plan calls for extensive IO preparations in peacetime using the full range of intelligence, surveillance, and reconnaissance capabilities to accurately map the computer networks and electronic signatures of potential adversaries. It calls for large efforts to characterize adversarial audiences as well as the adversarial decision makers themselves, in order to better target and exploit these using IO capabilities.

The Roadmap identifies the following benefits that will be accrued if its recommendations are achieved:

- Development of a common IO lexicon.
- More execution authority delegated to combatant commanders.

- Development of a trained and educated professional career force for IO.
- Centralized IO planning, integration, and analysis support from STRATCOM.
- Enhanced IO capabilities for the warfighter, to include:
    - Improved ability to disseminate powerful messages in support of adversary behavior modification.
    - Protection of networks with a real defense in depth strategy.
    - A robust offensive suite of capabilities to include full range electronic and computer network attack, with increased reliability through improved command and control, assurance testing, and refined tactics and procedures.

Critiques of Current State of Information Operations. The discussion of challenges and shortcomings in the Information Operations area include the following:

- No consensus on the definition of Information Operations or its contribution to overall mission accomplishment.
- Electronic Warfare policy and plant investment are outdated.
- OPSEC planning process is not widely applied and OPSEC, itself, is largely an "afterthought". Military Deception staff are not adequately trained prior to their assignments.
- Relationship of Public Affairs, Public Diplomacy, and PSYOP must be studied and clarified. PA must become more proactive. PSYOP authorities must be further decentralized.
- Information Operations career force and education require better planning and coordination for development.

Roadmap General Recommendations: The Roadmap's twelve recommendations are as follows:

1. Approve a common understanding of Information Operations.
2. Consolidate oversight and advocacy for Information Operations.
3. Delegate capabilities to combatant commanders.
4. Create a well trained and educated career work force.
5. Provide consolidated and comprehensive analytical support.
6. Correct immediate shortfalls and develop a long term defense in depth strategy for CND.
7. Mature CNA into a reliable warfighting capability.
8. Develop an electronic warfare investment strategy.
9. Increase psychological operations capabilities.
10. Clarify lanes in the road for PSYOP, Public Affairs, and Public Diplomacy.
11. Assign advocacy for operations security and military deception.
12. Improve transparency of Information Operations planning, programming, and budgeting, and execution system.

Return to Contents

Policy Actions to Implement the Roadmap to Date:

- IO Advocacy. DoDI 5143.01, "Undersecretary of Defense for Intelligence", issued 23 November 2005, designates the USD(I) as the principal staff assistant to the Secretary of Defense for Information Operations policy and integration activities.
- IO Career Force. DoDI 3608.11, "Information Operations Career Force" issued 4 November 2005 implemented the following:
    - Designated the Undersecretary of Defense for Intelligence (USD (I)) as the functional proponent for the IO career force
    - Specified that an interim IO career force of active and reserve military personnel be established, consisting of two categories of position: IO Planners and IO Capability Specialists (see glossary for definitions).
    - Allow for creation of guidance for enlisted and civilian IO career force in the future.
    - Required the USD (I) to monitor the accession, retention, and promotion rates for the IO career force.
- IO Education. DoDI 3608.12, "Joint Information Operations Education", (4 November 2005):
    - Specified that Joint IO education programs support the transformation of IO into a core military capability
    - Joint IO planners courses and graduate education programs expand the IO knowledge base in the services.
    - Designates USSTRATCOM as the operational advocate for joint IO education.
    - Requires National Defense University to have the Joint Forces Staff College (Norfolk, VA) develop and conduct a Joint IO Planner's Course.
    - Requires the Naval Postgraduate School (Monterey, CA) to establish an IO Center of Excellence and establish a graduate level joint IO education program.

DoD directives (DoDD) and instructions (DoDI) are available on line at:

www.dtic.mil/whs/directives/

Chairman of the Joint Chiefs of Staff instructions (CJCSI) and directives (CJCSD) are on line at:

www.dtic.mil/cjcs_directives/index.htm

Last Updated: December 2005

This Page Intentionally Blank

Return to Contents

Department of Defense Directive (DoDD) 3600.1 Information Operations

This section presents a synopsis of the current DRAFT of the revision of this Department of Defense Directive.

Purpose. Department of Defense Directive (DoDD) 3600.1, "Information Operations" is the *fundamental* document for both understanding and employing Information Operations (IO). It gives policy guidance to the Department of Defense for the management and implementation of IO throughout DoD.

Scope. As policy guidance, it defines terms; assigns responsibilities to officials, services, unified commands, and agencies; and provides the basis for the development of joint and service doctrine for IO. The term, "doctrine", as defined by Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms" (October, 2004) means: "*Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application*".

Information Operations (IO) Defined. IO is "The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own".

Use of IO.

- IO is to be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States.

- In peacetime, IO supports national objectives primarily by influencing adversary perceptions and decision-making. In crises short of hostilities, IO can be used as a flexible deterrent option to communicate national interest and demonstrate resolve. In conflict, IO may be applied to achieve physical and psychological results in support of military objectives. During post conflict or stability operations, IO continues to support national objectives and influence foreign perceptions.

- IO contributes to information superiority by both defending military decision- making from adversary attacks and by degrading an adversary's decision-making capability, and influencing other human activities thereby producing an information advantage. IO contributes directly to the national security strategy, which uses all elements of national power in a synchronized and coordinated manner to influence adversary perceptions and behavior.

- IO capabilities will be developed that can be employed in concert with various core, supporting, related, and intelligence capabilities to provide a fully integrated warfighting capability.

Core IO Capabilities.

IO employs five core capabilities to achieve desired Combatant Commander effects or prevent the enemy from achieving his desired effects: EW, CNO, PSYOP, MILDEC, and OPSEC. They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are interdependent and increasingly need to be integrated to achieve desired effects.

Supporting Capabilities.

Counterintelligence (CI) investigations, operations, collection, analysis, production, and dynamic functional services will be employed in support of appropriate IO activities to detect and mitigate foreign intelligence, hacker, and insider threats to DoD information and information systems.

Physical (kinetic) attack may be employed alone or integrated with non- kinetic attack options to influence or disrupt adversary decision-makers or groups and provide support for full spectrum dominance.

Physical Security will support IO by preventing unauthorized physical access to personnel, equipment, installations, material, and documents, and by safeguarding information and information systems against espionage, sabotage, damage, and theft.

Information Assurance (IA) will provide capabilities to protect and defend information and information systems. IA activities will be conducted independently to achieve these objectives or combined with specific CNO activities.

Combat Camera will provide to the Combatant Commander clear, timely, unaltered documentation of military operations. This documentation provides a source of video and still images that can be used to counter disinformation, misinformation, and propaganda.

Related Capabilities.

Public Affairs (PA), as a function of command, shall support the continuing public information and communication requirements of the Department. PA activities contribute to the broader U.S. Government (USG) communications effort by providing truthful, accurate and timely support to military members, their families, the media, and the public. This capability allows PA to help defeat adversary efforts to diminish national will, degrade morale, and turn world opinion against friendly operations. PA shall provide operational capabilities to communicate military objectives, counter misinformation and disinformation, deter adversary actions, and to maintain the trust and confidence of the U.S. population, as well as our friends and allies. Effective PA is based on credibility and shall not focus on directing or manipulating public actions or opinion.

Civil-Military Operations (CMO) activities shall support DoD informational objectives by influencing, developing, or controlling indigenous infrastructures in foreign operational areas, and can be an alternate means to communicate with the host nation and foreign public. CMO shall be performed by designated civil affairs personnel, by other military forces, or by a combination of both.

Defense Support to Public Diplomacy (DSPD) ensures the Department sends a coherent and compelling message in concert with other United States Government (USG) agencies. The prevalence of access to global communications requires a comprehensive and proactive USG communication strategy. The Department of State maintains the lead for public diplomacy with the Department of Defense in a supporting role. Through DSPD, the Department collaborates with other USG agencies for public diplomacy programs that directly support the Department of Defense's mission. It is critical that all DoD information activities be conducted in concert with the broader USG communications strategy and support the National Security Strategy.

Intelligence Support. Intelligence will be developed, consistent with the National Intelligence Priorities Framework, to provide data about adversary information systems or networks; produce political-military assessments; conduct human factors analysis; and provide indications and warning of adversary IO, including threat assessments.

Personnel. To achieve the objective of establishing IO as a core military competency, a cadre of IO Capability Specialists and IO Planners will be developed.

Security Cooperation Guidance. IO will be integrated into Security Cooperation Guidance for theater planning, as well as deliberate and contingency planning, to support national policy and strategy**.**

Further Policy Guidance:

- IO activities shall be coordinated and appropriately synchronized during peacetime and crisis actions and will include interagency coordination to ensure deconfliction with other agency programs, operations and activities.
- Tactics, techniques, procedures, and technologies will be shared among the DoD Components to fully facilitate synchronization and integration of IO.
- IO capabilities will be integrated into joint exercises and joint training regimes to the maximum extent possible.
- The DoD Information Operations and Space Executive Committee (IO & Space EXCOM) will serve as the senior corporate body advising the Secretary of Defense on issues relating to IO.

RESPONSIBILITIES. The following officials, commands, and agencies are tasked with the specific responsibilities indicated:

Under Secretary of Defense for Intelligence (USD(I)) :

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DoD IO policy and integration activities.
- Assess performance/responsiveness of DoD and Military Intelligence activities to support IO.
- Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.

Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) :

- Establish specific policies for the development and integration of EW as a core IO capability.
- Develop and maintain a technology investment strategy for development, acquisition, and integration of EW capabilities and IO threat countermeasures.
- Invest in and develop the science and technologies needed to support IO capabilities.

The Under Secretary of Defense for Policy (USD(P)):

- Provide DoD oversight of IO planning, execution, and related policy guidance including the establishment of an OSD review process to assess IO plans and programs
- Lead interagency coordination, exclusive of the IC, and international cooperation involving planning and employment of IO capabilities.

- Establish specific policy and oversight for development and integration of PSYOP as a core IO capability and DSPD as a related capability.

The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) :

- Develop policy and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), and others, as appropriate.
- Provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and joint training regimes.

The Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO) will:

- Establish specific policy for the development and integration of IA and Computer Network Defense (CND) as related to CNO as a core IO capability.
- Oversee and assess the efforts of the Heads of the DoD Components to plan, program, develop, and field IA and CND capabilities in support of CNO.

Assistant Secretary of Defense for Public Affairs will:

- Establish specific policy for the relationship of PA to IO.
- Oversee PA planning and coordination efforts as related to IO within DoD
- Oversee the development and conduct of appropriate training and education that defines PA's relationship to IO for public affairs and visual information personnel at the Defense Information School.

Commander, U.S. Strategic Command (CDRUSSTRATCOM):

Integrate and coordinate DoD IO core capabilities that cross geographic areas of responsibility or core IO areas.

Commander, U.S. Special Operations Command (CDRUSSOCOM)

- Integrate and coordinate DoD PSYOP capabilities to enhance interoperability and support USSTRATCOM's information operations responsibilities and other combatant commanders' PSYOP planning and execution.

- Support the other Combatant Commanders though joint employment of PSYOP and other special operations force IO capabilities.

- Employ other special operations force IO capabilities as directed.

The Secretaries of the Military Departments and CDRUSSOCOM

Develop IO doctrine and tactics, and organize, train, and equip for IO for their Title 10 (U.S. Code) and Major Force Program responsibilities.

Director, National Security Agency (NSA) will:

- Support IO planning and operations with Signals Intelligence, technology, and access.

- Support proposed IO courses of action with the intelligence gain/loss assessments and potential targeting strategies.
- Host and serve as Executive Secretary for the process to deconflict Department CNO activities with the IC.
- Assess the overall security posture of national security systems, and conduct CND activities as directed.
- Provide OPSEC assistance, products, and services.

Director, Defense Intelligence Agency (DIA) will:
Manage DoD all-source intelligence collection, analysis, and dissemination in support of IO intelligence requirements.

Heads of the DoD Components, as appropriate, will:

- Make Public Affairs officials aware of military plans and operations, and establish mutually supporting IO and PA efforts.
- Develop policy, doctrine, and the capabilities to execute IO across the range of military operations.
- Develop and conduct education, training, and exercise programs to provide for successful planning, integration, and execution of IO.

DEFINITIONS

Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. CND employs IA capabilities to respond to unauthorized activity within DoD information systems and computer networks in response to a CND alert or threat information. Note: CND also employs intelligence, counterintelligence, law enforcement and other military capabilities to defend DoD information and computer networks.

Computer Network Exploitation (CNE). Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

Computer Network Operations (CNO). Comprise CNA, CND, and related CNE enabling operations.

Defense Support to Public Diplomacy (DSPD). Those activities and measures taken by the DoD Components to support and facilitate the overt public diplomacy efforts of USG Departments and Agencies designed to promote U.S. foreign policy objectives.

Electronic Warfare (EW). Any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy.

Human Factors. The psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization.

Information. Facts, data, or instruction in any medium or form with context comprehensible to the user.

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Note: CND provides operational direction and guidance through global network operations and defense for employment of IA in response to a CND alert or specific threats.

Information Operations Specialists and Planners. Functional experts in one or more of the highly specialized core capabilities of CNO, EW, or PSYOP, who plan and execute the full spectrum of IO. IO planners shall understand basic principles associated with EW, CNO, and PSYOP, as well as understand an adversary's cultural and political context, in order to be capable of integrating IO effects into Combatant Commanders' plans and orders. Both IO Capability Specialists and IO Planners should be fully educated and trained to understand the planning principles associated with OPSEC and MILDEC.

Return to Contents

Information superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, and disseminate information.

Military Deception (MILDEC). Those measures designed to mislead an adversary by manipulation, distortion, or falsification to induce him to react in a manner prejudicial to his interests.

Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) Identify those actions that can be observed by adversary intelligence systems; b) Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Psychological Operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Public Affairs (PA). Those public information, command information and community relations activities directed toward both the external and internal audiences with interest in the Department of Defense. Effective PA is based on credibility, and shall not focus on directing or manipulating public actions or opinion.

Public Diplomacy. Those overt information activities of the USG designed to promote united foreign policy objectives by seeking to understand, inform and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad.

Security Cooperation. Those activities conducted with allies and friends, in accordance with Secretary of Defense Guidance, to: a) Build relationships that promote specified U.S. interests; b) Build allied and friendly capabilities for self-defense and coalition operations; c) Provide U.S. forces with peacetime and contingency access.

Final Department of Defense Directives (DoDD) on line:
DoDD 1000.1 thru 4999.99 -- http://www.dtic.mil/whs/directives/corres/dir1.html
DoDD 5000.1 thru 8999.99 -- http://www.dtic.mil/whs/directives/corres/dir2.html

Last Updated: December 2005

Return to Contents

Joint Information Operations Doctrine

JP 3-13 is currently under revision with a target publication date of early 2006.
The Executive Summary below is from the latest revision pending final approval.

Key doctrinal documents:
Joint Pub 3-13, *Information Operations*, XX Month 2006
Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare*, 7 February 1996
Joint Pub 3-51, *Joint Doctrine for Electronic Warfare*, 7 April 2000
Joint Pub 3-53, *Doctrine for Joint Psychological Operations*, 5 September 2003
Joint Pub 3-54, *Joint Doctrine for Operations Security*, 24 January 1997
Joint Pub 3-57, *Joint Doctrine for Civil-Military Operations*, 8 February 2001
Joint Pub 3-58, *Joint Doctrine for Military Deception*, 31 May 1996
Joint Pub 3-61, *Public Affairs*, 9 May 2005

Joint Pubs available at: http://www.dtic.mil/doctrine/index.html.

EXECUTIVE SUMMARY

- **Discusses the Information Environment and Its Relationship to Military Operations**

- **Discusses the Information Operations (IO) Core Capabilities Necessary to Successfully Plan and Execute IO to include Supporting and Related Capabilities in a Joint/Multinational Environment**

- **Aligns Joint IO Doctrine with the Transformational Planning Guidance as Specified by the Department of Defense IO Roadmap for Achieving Information Superiority on the Battlefield**

- **Provides an Organizational Framework for Integrating, Deconflicting, and Synchronizing IO Planning and Execution Activities for Supporting and Supported Combatant Command Staffs, National Intelligence Agencies, and Other Federal Agencies as Applicable**

- **Outlines Planning Considerations for Developing an IO Career Force through Joint Education, Training, Exercises, and Experimentation**

Military Operations and the Information Environment

To succeed, it is necessary for US forces to gain and maintain information superiority.

Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities.

Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

The purpose of this doctrine is to provide joint force commanders (JFCs) and their staffs guidance to help prepare, plan, execute, and assess IO in support of joint operations. The principal goal is to achieve and maintain information superiority for the US and its allies.

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.

Core, Supporting, and Related Information Operations Capabilities

Core capabilities.

IO consists of five core capabilities which are: PSYOP, MILDEC, OPSEC, EW, and CNO. Of the five, PSYOP, OPSEC, and MILDEC have played a major part in military operations for many centuries. In this modern age, they have been joined first by EW and most recently by CNO. Together these five capabilities, used in conjunction with supporting and related capabilities, provide the JFC with the principal means of influencing an adversary and other target audiences (TAs) by enabling the joint forces freedom of operation in the information environment.

Supporting capabilities.

Capabilities supporting IO include information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but can also serve other wider purposes.

Related capabilities.

There are three military functions, public affairs (PA), civilmilitary operations (CMO), and defense support to public diplomacy, specified as **related capabilities for IO**. These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting IO capabilities. However, their primary purpose and rules under which they operate must not be compromised by IO. This requires additional care and consideration in the planning and conduct of IO. For this reason, the PA and CMO staffs particularly must work in close coordination with the IO planning staff.

Intelligence and Communications System Support to Information Operations

Successful planning, preparation, execution, and assessment of. information operations (IO) demand detailed and timely intelligence.

Before military activities in the information environment can be planned, the current "state" of the dynamic information environment must be collected, analyzed, and provided to commanders and their staffs. This requires intelligence on relevant portions of the physical, informational, and cognitive properties of the information environment, which necessitates collection and analysis of a wide variety of information and the production of a wide variety of intelligence products.

Nature of IO intelligence requirements.

In order to understand the adversary or other TA decision-making process and determine the appropriate capabilities necessary to achieve operational objectives, commanders and their staffs must have current data. This includes relevant physical, informational, and cognitive properties of the information environment as well as assessment of ongoing IO activities.

Intelligence considerations in planning IO.

Intelligence Resources are Limited. Commanders and their intelligence and operations directorates must work together to identify IO intelligence requirements and ensure that they are given high enough priority in the commander's requests to the intelligence community (IC).

Collection Activities are Legally Constrained. The IC must implement technical and procedural methods to ensure compliance with the law. Additionally, intelligence may be supplemented with information legally provided by law enforcement or other sources.

Intelligence Support to IO Often Requires Long Lead Times. The intelligence necessary to affect adversary or other TA decisions often requires that specific sources and methods be positioned and employed over time to collect the necessary information and conduct the required analyses.

Information Environment is Dynamic. Commanders and their staffs must understand both the timeliness of the intelligence they receive and the differing potentials for change in the dimensions of the information environment.

Properties of the Information Environment Affect Intelligence. Collection of physical and electronic information is objectively measurable by location and quantity. Commanders and their staffs must have an appreciation for the subjective nature of psychological profiles and human nature.

Responsibilities and Command Relationships

Joint Staff.

The Chairman's responsibilities for IO are both general (such as those to establish doctrine, provide advice, and make recommendations) and specific (such as those assigned in DOD IO policy). The Operations Directorate of the Joint Staff (J-3) serves as the Chairman's focal point for IO and coordinates with the other organizations within the Joint Staff that have direct or supporting IO responsibilities. The IO divisions of the

Joint Staff J-3 provide IO specific advice and advocate Joint Staff and combatant commands' IO interests and concerns within DOD and interact with other organizations and individuals on behalf of the Chairman.

Combatant commands.

Commander, United States Strategic Command's (USSTRATCOM's) specific authority and responsibility to coordinate IO across area of responsibility (AOR) and functional boundaries does not diminish **the imperative for other combatant commanders to employ IO**. These efforts may be directed at achieving national or military objectives incorporated in theater security cooperation plans, shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations. It is entirely possible that in a given theater, the combatant commander will be supported for select IO while concurrently supporting USSTRATCOM IO activities across multiple theater boundaries.

Components.

Components are normally responsible for detailed planning and execution of IO. IO planned and conducted by functional components must be conducted within the parameters established by the JFC. At the same time, component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variations in the information environment. Component commanders determine how their staffs are organized for IO, and normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.

Subordinate joint force commanders.

Subordinate JFCs plan and execute IO as an integrated part of joint operations. Subordinate staffs normally share the same type of relationship with the parent joint force IO staff as the Service and functional components. **Subordinate JFC staffs may become involved in IO planning and execution to a significant degree**, to include making recommendations for employment of specific capabilities, particularly if most of the capability needed for a certain operation resides in that subordinate joint task force.

Organizing for joint IO.

Combatant commanders normally **assign responsibility for IO** to the **J-3**. When authorized, the director of the J-3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO. **The J-3 normally designates an IO cell chief** to assist in executing joint IO responsibilities. The primary function of the IO cell chief is to ensure that IO are integrated and synchronized in all planning processes of the combatant command staff and that IO aspects of such processes are coordinated with higher, adjacent, subordinate, and multinational staffs. To integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions, the IO cell chief normally leads an "IO cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. The organizational relationships between the joint IO cell and the organizations that support the IO cell are per JFC guidance.

Planning and Coordination

IO planning follows the same principles and processes established for joint operation planning.

The IO staff coordinates and synchronizes capabilities to accomplish JFC objectives. Uncoordinated IO can compromise, complicate, negate, or harm other JFC military operations, as well as other USG information activities. JFCs must ensure IO planners are fully integrated into the planning and targeting process, assigning them to the joint targeting coordination board in order to ensure full integration with all other planning and execution efforts. Other USG and/or coalition/allied information activities, when uncoordinated, may complicate, defeat, or render DOD IO ineffective. Successful execution of an information strategy also requires early detailed JFC IO staff planning, coordination, and deconfliction with USG interagency efforts in the AOR to effectively synergize and integrate IO capabilities.

Planning considerations.

IO planning must begin at the **earliest stage** of a JFC's campaign or operations planning and must be an integral part of, not an addition to, the overall planning effort. IO are used in all phases of a campaign or operation. The use of IO during early phases can significantly influence the amount of effort required for the remaining phases.

The use of IO in peacetime to achieve JFC objectives and to preclude other conflicts, requires an ability to integrate IO capabilities into a comprehensive and coherent strategy through the establishment of information objectives that in turn are integrated into and support the JFC's overall mission objectives. The combatant commander's theater security cooperation plan serves as an excellent platform to embed specific long-term information objectives.

IO planning requires early and detailed preparation. Many IO capabilities require long lead-time intelligence preparation of the battlespace (IPB). IO support for IPB development differs from traditional requirements in that it may require greater lead time and may have expanded collection, production, and dissemination requirements. Consequently, combatant commanders must ensure that IO objectives are appropriately prioritized in their priority intelligence requirements (PIRs) and requests for information (RFIs).

As part of the planning process, designation of release and execution authority is required. Release authority provides the approval for IO employment and normally specifies the allocation of specific offensive means and capabilities provided to the execution authority. Execution authority is described as the authority to employ IO capabilities at a designated time and/or place. Normally, the JFC is the one execution authority designated in the execute order for an operation.

IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.

Commander's intent and information operations.

The commander's vision of IO's role in an operation should begin before the specific planning is initiated. A commander that expects to rely on IO capabilities must ensure that IO related PIRs and RFIs are given high enough priority prior to a crisis, in order for the intelligence products to be ready in time to support operations. At a minimum, the commander's vision for IO should be included in the initial guidance. Ideally, commanders give guidance on IO as part of their overall concept, but may elect to provide it separately.

Measures of performance and measures of effectiveness.

Measures of performance (MOPs) gauge accomplishment of IO tasks and actions. **Measures of effectiveness (MOEs)** determine whether IO actions being executed are having the desired effect toward mission accomplishment: the attainment of end states and objectives. MOPs measure friendly IO effort and MOEs measure battlespace results. IO MOPs and MOEs are crafted and refined throughout the planning process.

Multinational Considerations in Information Operations

Every ally/coalition member can contribute to IO by providing regional expertise to assist in planning and conducting IO.

Allies and coalition partners recognize various IO concepts and some have thorough and sophisticated doctrine, procedures, and capabilities for planning and conducting IO. **The multinational force commander is responsible to resolve potential conflicts** between each nation's IO programs and the IO objectives and programs of the coalition. It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.

Integration requirements include clarification of allied and coalition partner's IO objectives; understanding of other nations' information operations and how they intend to conduct IO; establishment of liaison/deconfliction procedures to ensure coherence; and early identification of multinational force vulnerabilities and possible countermeasures to adversary attempts to exploit them.

Information Operations in Joint Education, Training, Exercises, and Experiments

A solid foundation of education and training is essential to the development of IO core competencies.

The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DOD. At the highest professional levels, senior leaders develop joint warfighting core competencies that are the capstone to American military power. The Services, United States Special Operations Command, and other agencies develop capabilities oriented on their core competencies embodied in law, policy, and lessons learned. At each level of command, a solid foundation of education and training is essential to the development of a core competency. Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation.

IO education considerations.

The IO career force should consist of both capability specialists (EW, PSYOP, CNO, MILDEC, and OPSEC) and IO planners. Both groups require an understanding of the information environment, the role of IO in military affairs, how IO differs from other information functions that contribute to information superiority, and specific knowledge of each of the core capabilities to ensure integration of IO into joint operations.

IO planners are required at both the component and the joint level.

Senior military and civilian DOD leaders require an executive level knowledge of the information environment and the role of IO in supporting DOD missions. Joint military training is based on joint policies and doctrine to prepare joint forces and/or joint staffs to respond to strategic and operational requirements deemed necessary by combatant commanders to execute their assigned missions.

IO training considerations.

IO training must support the IO career force and be consistent with the joint assignment process. Joint IO training focuses on joint planning-specific skills, methodologies and tools, and assumes a solid foundation of Service-level IO training.

The Services determine applicable career training requirements for both their IO career personnel and general military populations, based on identified joint force mission requirements.

CONCLUSION

This document provides the doctrinal principles for DOD employment of IO. It has been designed to provide overarching guidance in the planning and execution of IO in today's joint/multinational security environment. It's primary purpose is to ensure all of the capabilities comprising IO are effectively coordinated and integrated into our nation's warfighting capability against current and future threats.

Last Updated: January 2006.

Return to Contents

This Page Intentionally Blank

Return to Contents

Army Information Operations Doctrine

Key doctrinal documents:
FM 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, 28 November 2003

FM's are available at: http://www.adtdl.army.mil/ (in the processing of changing to new site).

Excerpts of Army Doctrine - FM 3-13

Introduction

Information operations (IO) encompass attacking adversary command and control (C2) systems (offensive IO) while protecting friendly C2 systems from adversary disruption (defensive IO). Effective IO combines the effects of offensive and defensive IO to produce information superiority at decisive points.

IO brings together several previously separate functions as IO elements and related activities. IO elements include the IO core capabilities, specified supporting capabilities, and related activities discussed in chapter 1. It also allows commanders to use all of them both offensively and defensively, as they deem appropriate. The assistant chief of staff (ACOS) G-7 has the coordinating staff responsibility for coordinating IO elements and related activities. This enables the G-7 to shape the information environment to friendly advantage and protect commanders and friendly C2 systems from adversary IO.

Offensive IO destroy, degrade, disrupt, deny, deceive, exploit, and influence adversary decision-makers and others who can affect the success of friendly operations. Offensive IO also target the information and information systems (INFOSYS) used in adversary decision-making processes.

Defensive IO protect and defend friendly information, C2 systems, and INFOSYS. Effective defensive IO assure friendly commanders an accurate common operational picture (COP) based not only on a military perspective, but also on nonmilitary factors that may affect the situation. An accurate COP is essential to achieving situational understanding. (See FM 6-0.) Most IO elements may be used either offensively or defensively. Effective IO requires integrating IO related activities—such as, public affairs and civil military operations—into IO as well.

Information Operations Doctrine

Commanders conduct (plan, prepare, execute, and assess) information operations (IO) to apply the information element of combat power. Combined with information management and intelligence, surveillance, and reconnaissance operations, effective IO results in gaining and maintaining information superiority. Information superiority creates conditions that allow commanders to shape the operational environment and enhance the effects of all elements of combat power. IO has two categories, offensive IO and defensive IO. Commanders conduct IO by synchronizing IO elements and related activities, each of which may be used either offensively or defensively. Army IO doctrine supports joint IO doctrine, supplementing it where necessary to meet the conditions of land operations.

Design of Army Information Operations

Information operations (IO) bring together several previously separate functions as IO elements and related activities. To provide unity of effort, IO is placed under a special staff officer, the assistant chief of staff G-7. … The G-7 has coordinating staff responsibility for IO. He does this by means of the G-7 section and IO cell. Placing responsibility for synchronizing the activities of the IO elements and related activities on one special staff officer helps commanders mass their effects to gain and maintain information superiority.

- **Information Environment**

  The *information environment* is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself (JP 3-13). It includes — • The worldwide interconnection of communications networks. • Command and control (C2) systems of friendly and adversary forces and other organizations. • Friendly, adversary, and other personnel who make decisions and handle information. Climate, terrain, and weapons effects (such as electromagnetic pulse or blackout) affect the information environment but are not part of it.

  Threat sources [include:] hackers, insiders, activist nonstate actors, terrorists, foreign IO activities, and information fratricide.

  Methods of attack include: unauthorized access, malicious software, electromagnetic deception, electronic attack, physical destruction, and perception management.

- **Information Superiority**

  The Army defines *information superiority* as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (FM 3-0). This definition differs slightly from the joint definition. While joint doctrine considers information superiority a capability, Army doctrine establishes it as an operational advantage. For Army forces, information superiority describes the degree of dominance that commanders have over the part of the information environment that affects their operations, and over the adversary. Commanders measure it in terms of information- based activities. Gaining and maintaining information superiority creates conditions that allow commanders to shape the information environment and enhance the effects of other elements of combat power. Commanders direct three interdependent contributors to achieve this goal:

  - Information management.
  - Intelligence, surveillance, and reconnaissance.
  - Information operations (including related activities).

  Information management is the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision-making. It uses procedures and information systems to collect, process, store, display, and disseminate information (FM 3-0). Information management (IM) consists of INFOSYS (see paragraph 1-6) and relevant information (RI).

  Intelligence, Surveillance, and Reconnaissance (ISR) is an enabling operation that integrates and synchronizes all battlefield operating systems to collect RI to facilitate the commander's decision-making.

  Information Operations Contributions. IM, IO, and ISR each have a different focus. ISR collects data and produces intelligence. IM disseminates and uses RI throughout the C2 system. IO applies that RI to protect the friendly C2 system, attack the adversary C2 system, and shape the information environment. All are essential to achieving and maintaining information superiority.

- **Aspects of Information Operations**

Information operations is the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making. (This definition supersedes the definition of IO in FM 3-0. It is consistent with joint initiatives.) [Editor's Note: It is also different from the current Joint definition.]

- **Elements of Information Operations**

IO are enabling operations that create and present opportunities for decisive operations. Commanders use both offensive IO and defensive IO simultaneously to accomplish the mission, increase their force effectiveness, and protect their organizations and systems. IO elements include core capabilities and supporting capabilities [see table below]. Commanders conduct IO through a combination of these elements and related activities.

The elements of IO are not organizations. They are independent activities that, when taken together and synchronized, constitute IO. Commanders decide which IO elements are appropriate to accomplish the mission. All elements may not be required for each operation.

With the possible exceptions of computer network operations (CNO), CNA, computer network defense (CND) and computer network exploitation (CNE), no IO element is new. What is new is bringing these elements/related activities together as components of the information element of combat power. IO focuses efforts that before were diffuse. A single staff officer—the G-7—is assigned authority and responsibility for these previously separate activities. This allows commanders to mass the effects of the information element of combat power.

Core	Supporting
• Electronic warfare • Computer network operations o Computer network attack o Computer network defense o Computer network exploitation • Psychological operations • Operations security • Military deception	• Physical destruction • Information assurance • Physical security • Counterintelligence • Counterdeception • Counterpropaganda

Information Operations Elements

Editor's Note: Subordinate elements of CNO are indented in the table for clarity.

IO related activities include but are not limited to public affairs (PA) and CMO. Although FM 3-13 discusses only these two, any activity that contributes to gaining and maintaining information superiority (for example, an operation in support of diplomatic efforts conducted by special operations forces) may be considered an IO related activity.

- **Army-Joint Information Operations Relationships**

IO, by their nature, are joint operations. Each Service component contributes to an integrated whole synchronized by the joint force headquarters. …. The IO cell at joint force headquarters deconflicts and synchronizes joint force IO. All Service components are represented. The joint force IO cell synchronizes all the Service-specific IO elements/related activities to achieve unity of effort supporting the joint force. Army forces submit requests for IO support from joint force or higher echelons through the senior Army headquarters to the joint force IO cell.

- **Offensive Information Operations**

  The Army defines ***offensive information operations*** as the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision-makers or to influence others to achieve or promote specific objectives (FM 3-0). The Army definition deletes a sentence in the joint definition that lists IO elements associated with offensive IO. Army doctrine allows commanders to use all IO elements offensively.

  Offensive IO facilitates seizing and retaining the initiative by creating a disparity between the quality of information available to friendly forces and that available to adversaries. The following effects create this information advantage:

  - **Destroy**. *Destroy* is to damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt (FM 3-90). Destruction is most often the use of lethal and nonlethal means to physically render adversary information useless or INFOSYS ineffective unless reconstituted.
  - **Disrupt**. *Disrupt* is a tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt his timetable, or cause his forces to commit prematurely or attack in a piecemeal fashion (FM 3-90). *Disrupt*, in information operations, means breaking or interrupting the flow of information between selected C2 nodes.
  - **Degrade**. *Degrade*, in information operations, is using nonlethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems, and information collection efforts or means. Offensive IO can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
  - **Deny**. *Deny*, in information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decision-making. Effective denial leaves opponents vulnerable to offensive capabilities. OPSEC is the primary nonlethal means of denial. It applies throughout the spectrum of conflict.
  - **Deceive**. *Deceive* is to cause a person to believe what is not true. Military deception (MD) seeks to mislead adversary decision-makers by manipulating their understanding of reality. Successful deception causes them to believe what is not true.
  - **Exploit**. *Exploit*, in information operations, is to gain access to adversary command and control systems to collect information or to plant false or misleading information.
  - **Influence**. *Influence* is to cause adversaries or others to behave in a manner favorable to Army forces. It results from applying perception management to affect the target's emotions, motives, and reasoning. Perception management also seeks to influence the target's perceptions, plans, actions, and will to oppose friendly forces.

- **Defensive Information Operations**

  The Army defines ***defensive information operation****s* as the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes (FM 3-0). The Army definition deletes a sentence in the joint definition that lists IO elements associated with defensive IO. Army doctrine allows commanders to use all IO elements defensively.

Defensive IO seeks to limit the vulnerability of C2 systems to adversary action and to prevent enemy interference with friendly information and INFOSYS. Defensive IO effects include: **protection, detection, restoration, and response**.

- **Protection.** *Protection* is all actions taken to guard against espionage or capture of sensitive equipment and information. In IO, protection occurs at the digital perimeter to control access to or mitigate the effects of adversary access to friendly decision-makers and INFOSYS.
- **Detection.** *Detection* is to discover or discern the existence, presence, or fact of an intrusion into information systems. Detection is the identification of adversary attempts to gain access to friendly information and INFOSYS.
- **Restoration.** *Restoration* is to bring information systems back to their original state. Restoration is reestablishment of essential capabilities of INFOSYS damaged by enemy offensive IO.
- **Response.** *Response* in information operations is to react quickly to an adversary's information operations attack or intrusion. Timely identification of adversaries, their intent and capabilities, is the cornerstone of effective response to adversary offensive IO.

- **Relationship of Offensive and Defensive Information Operations**

  Commanders synchronize offensive and defensive IO to produce complementary and reinforcing effects (see FM 3-0). Offensive IO supports the decisive operation, while defensive IO protects friendly force critical assets and centers of gravity. Conducting offensive and defensive IO independently detracts from the efficient employment of IO elements.

- **Information Operations Across the Spectrum of Conflict**

The national security and national military strategies establish an imperative for engagement (see FM 1). Engagement involves the nation exercising the instruments of national power—diplomatic, informational, military, and economic—to shape the security environment. … Throughout the spectrum of conflict, commanders conduct IO to apply the information element of combat power. In all situations, Army forces do not act in isolation. Almost all operations are joint; most are interagency as well.

- **Peace.** During peace, commanders conduct IO to shape the strategic environment or to prepare for operations during crisis and war. Normally IO are part of a combatant commander's theater engagement plan. The majority of peacetime preparation is done at home station or during training exercises.

- **Crisis.** During crises, Army forces conduct IO based on existing contingency plans or a crisis action plan (see JP 5-0). A potential or actual contingency requires commanders at all echelons to gather additional information and refine their contingency plans based on a specific AO or target set. Geographic combatant commanders may use the relationships and conditions in the information environment created during peace to influence potential adversary decision-makers to act in ways that will resolve the crisis peacefully.

- **War.** During war, commanders conduct IO to synchronize the information element of combat power with the other elements of combat power. Well-synchronized offensive IO can cripple not only adversary military power but also adversary civilian decision-making capability. Commanders and staffs follow the military decision-making process to plan IO that accomplishes the commander's intent and concept of operations.

- **The G-7 Section and the Information Operations Cell**

  The G-7 has coordinating staff responsibility for IO. He does this by means of the G-7 section and IO cell. The G-7 section has assigned officers and NCOs responsible for IO current operations, IO planning and IO targeting... The G-7 coordinates IO related activities of other staff officers through the IO cell.

The IO cell, located in the main command post, brings together representatives of organizations responsible for all IO elements and related activities. Related activities include any organizations able to contribute to achieving IO objectives. PA and CMO are always related activities; commanders may designate others. The IO cell also includes representatives of special and coordinating staff sections, as the mission requires. All battlefield operating systems are represented. The primary function of an IO cell is to synchronize IO throughout the operations process. In corps and divisions, the G-7 section forms its nucleus. In Army service component commands (ASCCs), the plans, current operations, and effects control divisions—under the deputy chief of staff for operations—coordinate IO. The ASCC ensures Army IO supports the theater IO campaign plan. If another headquarters is designated as the ARFOR, that headquarters assumes this responsibility

Information Operations Elements and Related Activities

The core and supporting IO elements are similar to the battlefield operating systems. They are independent activities that, when taken together and synchronized, constitute IO.

- **Core Elements**

Core IO elements are operations security (OPSEC), psychological operations (PSYOP), military deception (MD), electronic warfare (EW) and computer network operations (CNO). ***Computer network operations*** **comprise computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations.**

PSYOP, MD and OPSEC are employed to influence adversary decision-makers or groups while protecting friendly decision-making. EW and CNO are employed to affect or defend the electromagnetic spectrum, information systems (INFOSYS), and information that support decision-makers, weapon systems, command and control (C2), and automated responses.

- **Operations Security**

The Army defines *operations security* as a process of identifying essential elements of friendly information and subsequently analyzing friendly actions attendant to military operations and other activities to --

  - Identify those actions that can be observed by adversary intelligence systems.
  - Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive essential elements of friendly information time to be useful to adversaries.
  - Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

- **Psychological Operations**

Psychological operations are planned operations that convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives (JP 3-53).

- **Military Deception**

Military deception comprises actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-58). It is used to make an adversary more vulnerable to the effects of friendly force weapons, maneuver, and operations.

- **Electronic Warfare**

Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-51). … The three major components of EW are electronic protection (EP), electronic warfare support (ES), and electronic attack (EA).

  - **Electronic Protection**. *Electronic protection* is that division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability (JP 3-51).

  - **Electronic Warfare Support**. *Electronic warfare support* is that division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations.

  - **Electronic Attack**. *Electronic attack* is that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

- **Computer Network Operations**

Computer network operations comprise computer network attack, computer network defense, and related computer network exploitation enabling operations. CNO is not totally applicable at the tactical level. CNO is applicable at echelons above corps.

  - 2-31. *Computer network attack* is operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (JP 3-13).

  - *Computer network defense* consists of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction (JP 3-51). It includes all measures to detect unauthorized network activity and adversary CNA and defend computers and networks against it.

  - *Computer network exploitation* consists of enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

- **Supporting Elements**

The supporting IO elements are physical destruction, IA, physical security, counterintelligence, counterdeception, and counterpropaganda.

- **Physical Destruction**

  Physical destruction is the application of combat power to destroy or degrade adversary forces, sources of information, command and control systems, and installations. It includes direct and indirect fires from ground, sea, and air forces. Also included are direct actions by special operations forces.

- **Information Assurance**

  Information assurance comprises information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (JP 3-13).

  - *Availability* means timely, reliable access to data and services by authorized users. Available INFOSYS operate when needed.
  - *Integrity* means protection from unauthorized change, including destruction. INFOSYS with integrity operate correctly, consistently, and accurately.
  - *Authentication* means certainty of user or receiver identification and authorization to receive specific categories of information.
  - *Confidentiality* means protection from unauthorized disclosure.
  - *Nonrepudiation* means proof of message receipt and sender identification, so neither can deny having processed the data.

- **Physical Security**

  Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-13). Effective physical security ensures the availability of INFOSYS used to conduct operations**.**

- **Counterintelligence**

  Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 3-13). The CI mission is to detect, identify, assess, counter, neutralize, or exploit hostile intelligence collection.

- **Counterdeception**

  Counterdeception consists of efforts to negate, neutralize, diminish the effects of, or gain the advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations (JP 3-13). Counterdeception contributes to situational understanding and defensive IO by protecting friendly C2 systems and decision-makers from adversary deception. Its goal is to make friendly decision-makers aware of adversary deception activities so they can formulate informed and coordinated responses.

- **Counterpropaganda**

  Counterpropaganda consists of programs of products and actions designed to nullify propaganda or mitigate its effects (FM 3-05.30). It is directed toward the target of adversary propaganda. Counterpropaganda degrades the harmful influence of adversary PSYOP on friendly forces and other audiences (see JP 3-53; FM 3-05.30; FM 33-1-1). … Counterpropaganda includes countering adversary misinformation, disinformation, and opposing information.

- **Related Activities**

  Related activities include, but are not limited to, [Public Affairs] PA and [Civil Military Operations] CMO.

  - **Public Affairs**

    Public affairs are those public information, command information, and community relations' activities directed toward both the external and internal publics with interest in the Department of Defense (JP 3-61). (Army doctrine uses the term *internal information* in place of *command information*.) PA information is credible. It makes available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy.

  - **Civil Military Operations**

    Civil military operations are activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational United States objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government.

Tactics, Techniques, and Procedures

Like all military operations, information operations follow the operations process: planning, preparation, execution, and continuous assessment.

Planning Information Operations

- **Information Operations Planning Concepts**

  Planning is the means by which the commander envisions a desired outcome, lays out effective ways of achieving it, and communicates to his subordinates his vision, intent, and decisions, focusing on the results he expects to achieve. … Commanders use the IO mission statement, IO concept of support, IO objectives, and IO tasks to describe and direct IO.

  - The *information operations mission statement* is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it.

  - The *information operations concept of support* is a clear, concise statement of where, when, and how the commander intends to focus the information element of combat power to accomplish the mission.

  - *Information operations objectives* are clearly defined, obtainable aims that the commander intends to achieve using IO elements/related activities.

- *Information operations tasks* are tasks developed to support accomplishment of one or more information operations objectives. An IO task addresses only one IO element/related activity.

The most important IO planning product is the IO subparagraph or IO annex of the operation plan (OPLAN) or operation order (OPORD) (see appendix D). The IO annex usually includes an IO execution matrix and IO assessment matrix as appendixes.

- **Receipt of Mission**

Upon receipt of a mission, either from higher headquarters or from the commander, the commander and staff perform an initial assessment. Based on this assessment, the commander issues initial guidance and the staff prepares and issues a WARNO. During the time between receiving the commander's initial guidance and issuing the WARNO, the staff performs [the following] receipt of mission actions:

- Participates in the commander's initial assessment.
- Receives the commander's initial guidance.
- Reviews the IO estimate.
- Prepares for future planning.

- **Mission Analysis**

During mission analysis, the staff defines the tactical problem and begins to determine feasible solutions. Mission analysis consists of 17 tasks. Many of them are performed concurrently. The mission analysis products are the restated mission, initial commander's intent, commander's guidance, and at least one WARNO. … The staff performs the following tasks during mission analysis:

- Analyze the higher headquarters order.
- Conduct IPB.
- Determine specified, implied, and essential tasks.
- Review available assets.
- Determine constraints.
- Identify critical facts and assumptions.
- Conduct risk assessment.
- Determine initial commander's critical information requirements.
- Determine the initial ISR annex.
- Plan use of available time.
- Write the restated mission.
- Conduct a mission analysis briefing.
- Approve the restated mission.
- Develop the initial commander's intent.
- Issue the commander's guidance.
- Issue a WARNO.

  - Review facts and assumptions.

- **Course of Action Development**

  After the mission analysis briefing, the staff begins developing COAs for analysis and comparison based on the restated mission, commander's intent, and planning guidance. During COA development, the staff prepares feasible COAs that integrate the effects of all combat power elements to accomplish the mission. Based on the initial IO mission statement, the G-7 develops a distinct IO concept of support, IO objectives, and IO tasks for each COA [while performing the following actions].

  - Analyze relative combat power
  - Generate options
  - Array initial forces
  - Develop the concept of operations
  - Recommend headquarters [for command and control]
  - Prepare COA statements and sketches

- **Course of Action Analysis (War-gaming)**

  COA analysis (war-gaming) identifies which COA accomplishes the mission with minimum casualties while best positioning the force to retain the initiative. War-gaming is a disciplined process that staffs use to envision the flow of battle. Its purpose is to stimulate ideas and provide insights that might not otherwise be discovered. Effective war-gaming allows the staff to test each COA, identify its strengths and weaknesses, and alter it if necessary.

- **Course of Action Comparison**

  During COA comparison, the staff compares feasible courses of action to identify the one with the highest probability of success against the most likely adversary COA and the most dangerous adversary COA. Each staff section evaluates the advantages and disadvantages of each COA from the staff section's perspective, and presents its findings to the staff. The staff outlines each COA in terms of the evaluation criteria established before the war game and identifies the advantages and disadvantages of each with respect to the others.

- **Course of Action Approval**

  After completing the COA comparison, the staff identifies its preferred COA and recommends it to the commander—in a COA decision briefing, if time permits. The concept of operations for the approved COA becomes the concept of operations for the operation itself. The IO concept of support for the approved COA becomes the IO concept of support for the operation. Once a COA is approved, the commander refines the commander's intent and issues additional planning guidance.

- **Orders Production**

  Based on the commander's decision and final guidance, the staff refines the approved COA and completes and issues the OPLAN/OPORD. Time permitting, the staff begins planning branches and sequels.

Preparing for Information Operations

Preparation for information operations (IO) includes actions performed before execution to improve the ability to conduct both offensive and defensive IO. It includes revising and refining plans and orders, assessment, force protection, coordination and liaison, rehearsals, task organization and movements, preoperation checks and inspections, logistic preparations, and integration of new soldiers and IO-capable units. When a unit executing one mission receives a warning order for a follow-on mission, it begins preparing for that mission while executing its current mission.

Executing Information Operations

The complexity of information operations (IO) execution stems from IO's multiple elements with their diverse operational capabilities and requirements. The wide variance in the time IO elements need to achieve effects and the coordination required between echelons add complexity. Well-executed IO results in confused and demoralized adversary leaders and soldiers. It produces psychologically and electronically isolated adversary units incapable of mounting coordinated efforts. Often, adversary commanders are severed from their subordinates and powerless to counter Army force actions at the decisive point. … [Effective] IO execution {includes]: staff coordination, assessing IO, decision-making, and other IO-related considerations.

Last Updated: November 2004.

Return to Contents

Marine Corps Information Operations Doctrine

Key doctrinal documents:

- Marine Corps Order 3430.8, *Policy for Information Operations*, 19 May 1997 (Under revision)
- MCWP 3-40.4, *MAGTF Information Operations*, 9 Jul 2003.
- MCWP 3-40.2, *Information Management*, 24 Jan 2002. (Focuses on defensive measures).
- MCWP 3-40.5, *Electronic Warfare*, 10 Sep 2002.
- MCWP 3-40.6 Psychological Operations (Dual Designated w/ Army)
- MCRP 3-40.6A PSYOP tactics, techniques, and procedures (Dual Designated)
- MCRP 3-40.6B Tactical PSYOP TTP's (Dual Designated w/ Army)

Excerpts from the forthcoming "Small Wars/21st Century" (MCRP 3-33.3B)

"The focus of IO is on the individual decision makers and the decision making process. IO is the ability to adversely influence enemy decision making processes while enhancing and protecting their own. Therefore, for IO to be successful, it demands an ability to understand people, cultures, and motivations. In the context of maneuver warfare, IO attempts to disrupt the observe, orient, decision, action (OODA) loop of the enemy affecting his ability to act by causing the enemy to receive information that is inaccurate, incomplete, or received at an inopportune time."

"IO covers the entire spectrum of warfare and is a key capability in small wars. Peacetime IO can be used to influence our adversaries through regional engagement and influence operations to help shape the strategic environment. Additionally, it can be used to impart a clearer understanding and perception of our mission and its purpose. In the pre-crisis stage, IO can help deter adversaries from initiating actions detrimental to the interests of the United States or its allies. Carefully conceived, coordinated, and executed, IO can make an important contribution to defusing crises; reducing the period of confrontation; and enhancing diplomatic, economic, military, and social activities, thereby forestalling and possibly eliminating the need to employ physical force. In the crisis stage, IO can be a force multiplier. During combat operations, IO can help shape the battlespace and prepare the way for future combat actions to accomplish the MAGTF's (Marine Air Ground Task Force) objectives. Once the crisis is contained, IO may help restore peace and order, and allow the successful termination of military operations."

"The MAGTF may target hostile forces and their supporters in a given area with one message, and a different message in another area. It may also be necessary to influence the neutral component of the population to influence them in a positive way to support our allies and coalition partners. Obviously, the impact of each message is dependent upon a very nuanced understanding of current perceptions."

"By operationalizing IO, and expertly employing defensive and offensive IO tactics, techniques and procedures, we can gain the initiative and achieve an informational advantage over our opponents. IO is the cumulative effect of distinct functions integrated in order to create synergistic effects and act as a force multiplier. These functions, when combined with accurate and timely intelligence, form the basis of IO."

Excerpts of Marine Corps Doctrine - MCWP 3-40.4 (9 Jul 2003)

Information Operations in Support of Expeditionary Warfare

"Marine Corps information operations (IO) support maneuver warfare through actions that use information to deny, degrade, disrupt, destroy or influence an adversary commander's methods, means or ability to C2 his forces and to inform target audiences through informational activities. IO enhance the ability of the MAGTF to project power during peace and war. They complement and facilitate the traditional use of military force but in some instances may stand alone as a deterrent option. IO support the integration of situational awareness, operational tempo, influence, and power projection to achieve advantage."

IO is an integrating concept that facilitates the warfighting functions of C2 (command and control), fires, maneuver, logistics, intelligence, and force protection. IO is not simply another "arrow" in the MAGTF commander's quiver. IO is a broad-based capability that "makes the bow stronger."

IO is multi-disciplined. Capabilities relevant to IO include, but are not limited to, the five core capabilities of IO, -- psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), electronic warfare (EW), computer network operations (CNO), as well as the supporting and related capabilities. These include public affairs (PA), civil-military operations (CMO), and combat camera (COMCAM). IO conducted by MAGTFs support battlespace shaping, force enhancement, and force protection activities. IO will enhance the ability of the MAGTF to project power during peace and war, complementing and facilitating the traditional use of military force.

MAGTFs will execute IO to enable and enhance their ability to conduct military operations consistent with the Marine Corps' capstone concept, *Expeditionary Maneuver Warfare (EMW)*. The MAGTF can support joint and multinational enabling by serving as an adaptive cornerstone force-bringing flexible command, control, communications, computers, and intelligence (C4I) systems that allow a joint or coalition force to be assembled in an expeditionary environment. Marines also bring unique capabilities, such as the electronic attack (EA)-6B Prowler aircraft and the Mobile Electronic Warfare Support System, adding to the combat power of the joint force. The Communications Emitter Sensing and Attack System (CESAS) is taking over some of the EA mission for the Radio Battalions. The MAGTF will frequently rely on national level agencies and other service components for certain offensive and defensive IO related capabilities.

IO can increase strategic agility by utilizing the reach back capability of MAGTF command, control, communications, and computers (C4) systems thus allowing the MAGTF to draw upon information sources outside its area of operations. IO can extend operational reach through informational and media activities that unify power projection with influence projection. IO can increase tactical flexibility by providing the MAGTF commander with a range of both lethal and nonlethal options. Finally, IO can enhance support and sustainment by enabling power projection against distant targets without increasing the MAGTF's footprint ashore.

Principles

- *IO is an integral function of the MAGTF.*
- *MAGTF IO is focused on the objective.*
- *The MAGTF commander's intent and concept of operations determine IO targets and objectives.*

- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands*
- *MAGTF IO is supported by the total force.*
- *Many different capabilities and activities must be integrated to achieve a coherent IO strategy.*
- *Intelligence support is critical to the planning, execution, and assessment of IO.*

Offensive and Defensive Operations

- **Offensive IO** objectives must be clearly established. They must support overall national and military objectives and include identifiable indicators of success. Selection and employment of specific offensive capabilities against an enemy must be appropriate to the situation. Offensive IO may be the main effort, a supporting effort or a phase in the MAGTF operation. Offensive IO objectives include the following:

    - Influence the adversary commander's estimate of the situation.
    - Slow the adversary's tempo of operations.
    - Degrade the adversary commander's decision cycle for planning and executing operations.
    - Disrupt the adversary commander's ability to generate and focus combat power.

- **Defensive IO** ensure timely, accurate, and relevant information access while denying the enemy the opportunity to exploit friendly information and information systems for its own purposes. Since it is a practical impossibility to defend every aspect of the infrastructure and every information process, defensive IO provide the essential and necessary protection and defense of information and information systems upon which the MAGTF depends to conduct operations and achieve objectives.

    The basis for defensive IO planning is the conduct of OPSEC, C4 vulnerability analysis, identification and protection of essential elements of friendly information, and the generation of the restricted frequency list.

    The objectives of defensive IO include the following:

    - Sustain the MAGTF commander's freedom of action.
    - Reduce the adversary's ability to affect friendly C2.
    - Minimize friendly C2 system vulnerabilities to adversary C2 attack through the employment of adequate physical, electronic, information, and OPSEC measures.
    - Minimize friendly mutual interference on friendly C2 and unintended third parties throughout the electromagnetic spectrum.
    - Minimize the effects of adversary perception management activities.

Operational Focus. The primary focus of MAGTF IO activities will be at the operational and tactical levels of war.

Staff Responsibilities

- The G-3/S-3 is responsible for IO. The future operations section is responsible for overseeing the planning and coordination of the IO effort. The MAGTF IO officer, within G-3/S-3 future operations, is responsible for:

    - The broad integration and synchronization of IO efforts.
    - Responding directly to the G-3/S-3 for MAGTF IO.

    - Ensuring that the IO cell provides input to the operational planning team (OPT) during planning to ensure coordinated operations.
    - Preparing the IO appendix to the operation order (OPORD).
    - Overseeing the core personnel within the IO cell as well as augmentees from external agencies.
    - Ensuring that all IO matters are coordinated within the MAGTF staff, higher headquarters, and external agencies.

- The electronic warfare officer (EWO) integrates EW operations through the EW coordination center or the IO cell when established.

Information Operations Cell

The IO cell is a task-organized group that is established within a MAGTF and/or higher headquarters to integrate a variety of separate disciplines and functions pertaining to IO for the command. A fully functioning IO cell integrates a broad range of potential IO actions and related activities that contribute to accomplishing the mission. IO integration requires extensive planning and coordination among all the elements of the staff. The IO cell, when established, is a mechanism for achieving that coordination.

Information Operations Capabilities

- **Overview.** IO include all action taken to affect enemy information and information systems while defending friendly information and information systems. IO are focused on the adversary's key decision-makers. IO are conducted during all phases of an operation, across the range of military operations, and at every level of war.

Note: The following *descriptions* are presented vice the *definitions* which in most cases are the respective Joint definitions found in JP 1-02.

- **Deception.** Military deception targets enemy decision makers by targeting their intelligence collection, analysis, and dissemination systems. Deception requires a thorough knowledge of adversaries and their decision making processes. Military deception is focused on achieving a desired behavior, not simply to mislead. The purpose is to cause adversaries to form inaccurate impressions about friendly force capabilities or intentions by feeding inaccurate information through their intelligence collection or information assets. The goal is to cause the adversary to fail to employ combat or support units to their best advantage.

- **Electronic warfare** is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or the attack the enemy. The three major subdivisions within EW are: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). (JP 1-02)

- **Operational Security.** OPSEC is the key to information denial. It gives the commander the capability to identify indicators that can be observed by adversary intelligence systems. These indicators could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or COAs that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate or reduce indications and other sources of information, which may be exploited by an adversary, to an acceptable level.

- **Psychological Operations** (PSYOP) are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. (JP 1-02). See also MCWP 3-40.6 (formerly FMFM 3-53), *Psychological Operations*….Note: The Marine Corps is standing up a Tactical PSYOP Team (TPT) that will be attached to each Marine Expeditionary Unite

(MEU). It will consist of one officer and three enlisted, and concerned solely with tactical PSYOP. If requested, external PSYOP support at eschelons higher than the MEU may be provided by the US Army's 4th Psychological Operations Group (POG).

- **Computer Network Operations.** CNO support C2 by facilitating the decision making process by providing communication and information systems that are reliable, secure, timely, and flexible. CNO protect information and information processes through computer network defense and IA activities. CNO may also be used to attack or exploit an adversary's information systems through computer network attack or exploitation. The Marine cryptologic support battalion or the RadBn may be tasked to support CNO activities. While the MAGTF does not have a computer network attack (CNA) force, it must be aware of available joint capabilities. Additionally, the MAGTF must be prepared to defend against the CNA threat posed by the adversary.

- **Physical Attack** applies friendly combat power against the enemy. It reduces enemy combat power by destroying enemy forces, equipment, installations, and networks. Within IO, physical destruction is the tailored application of combat power to achieve desired operational effects.

- **Information Assurance.** IA is information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP-02). IA capabilities include information security.

- **Physical Security** contributes directly to information protection. Information, information-based processes, and information systems—such as C4 systems, weapon systems, and information infrastructures— are protected relative to the value of the information they contain and the risks associated the compromise or loss of information.

- **Counterintelligence.** The principal objective of CI is to assist with protecting friendly forces. CI is the intelligence function concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism. CI enhances command security by denying adversaries information that might be used against friendly forces and to provide protection by identifying and neutralizing espionage, sabotage, subversion or terrorism efforts. CI provides critical intelligence support to command

- **Public Affairs.** The PA mission is to provide timely, accurate information to Marines and the general public and to initiate and support activities contributing to good relations between the Marine Corps and the public. PA expedites the flow of accurate and timely information to internal and external audiences. In peacetime, PA provides Marine and the general public with information that increases public understanding of the Marine Corps' roles and missions. PA efforts can have positive as well as negative impacts within the battlespace and the consequences of its use can have a strategic effect on the mission.

- **Civil-Military Operations.** Each military operation has a civil dimension. The civil dimension requires that commanders consider how their actions affect, and are affected by, the presence of noncombatants. Accordingly, CMO have become an integral element of military operations. Through careful planning, coordination, and execution, CMO can help the MAGTF win by shaping the battlespace, enhancing freedom of action, isolating the enemy, meeting legal and moral obligations to civilians, and providing access to additional capabilities.

Intelligence Support to Planning. Intelligence provides the essential basis for planning IO through the following considerations:

- The adversary commander's freedom of action and the freedom of action allowed to subordinates including adversary perceptions of the situation and developments.
- Adversary IO capability, intent, morale, and vulnerability to offensive IO.
- C2 aspects such as key personnel, target audiences, headquarters, communications nodes, databases or intelligence collection systems. C2 nodes that appear in more than one adversary COA should be highlighted for targeting.
- Assessments of friendly vulnerability to adversary IO.

Similar intelligence products support each of the various IO capabilities; for example, OPSEC, PSYOP, deception, EW, CNO, CI, physical attack, physical security, IA. The intelligence requirements for each capability are interrelated.

Updated: December 2005.

Navy Information Operations Doctrine

Key doctrine and tactics, techniques, and procedures

- NWP 3-13, *Navy Information Operations*, June 2003
- NTTP 3-13.1, *Theater and Campaign Information Operations*, January 2002
- NTTP 3-13.2, *Navy IO Warfare Commander's Manual*, June 2001 (updated December 2003)
- Core Capabilities:
    - NTTP 3-51.1, *Navy Electronic Warfare (draft)*
    - TACMEMO 3-13.2-03, *Psychological Operations for Navy Planners,* October 2003
    - NTTP 3-54.3, *Navy Operations Security*, July 2005
    - NTTP 3-58.1, *Multi-Service Military Deception* (draft)
    - NTTP 3-58.2, *Navy Military Deception*, August 2003 (updated December 2005)
    - NTTP 3-13.1.15, Multi-Service *Reprogramming,* January 2003
    - TACMEMO 3-13.1-03, *Computer Network Defense for Strike Groups*, October 2003

- **NWPs, NTTPs, and TACMEMOs are available at:** http://www.nwdc.navy.smil.mil under the Navy Warfare Library link.

Summary of Navy IO Doctrine and Concepts

Introduction

The United States (U.S.) has experienced a shift from strictly symmetric, or force-on-force, warfare to more asymmetric warfare and military operations other than war (MOOTW). Today's adversaries rely on asymmetric operations such as terrorism, disinformation, and propaganda campaigns to circumvent or undermine U.S. and allied strengths and exploit friendly vulnerabilities. IO has evolved from command and control warfare (C2W) as new capabilities and vulnerabilities for affecting the adversary and protecting friendly decision makers emerge. Concepts and methods of organizing, planning, and conducting IO are refined on a routine basis during exercises and daily operations. Rapid advances in information technology provide today's military with unparalleled abilities to collect, process, and disseminate information. Technological advances have also increased the commander's vulnerability as a target for adversary information collection, shaping, and attack. IO is increasingly important for managing vulnerabilities and countering emergent threats.

Information Operations Fundamentals

Maritime Power Projection

No one can predict with certainty the future security environment, but emerging trends require that the Navy focus on the littorals and the land beyond. The Navy must remain expeditionary in nature, controlling the sea and moving around the globe to support U.S. national interests. The vision for the future is a Navy and Marine Corps team that will maintain a robust and credible forward presence. These forces provide a framework that complements other instruments of national power to build stability and favorably shape areas overseas.

Forward presence, combined with knowledge superiority within the environment, will achieve the ultimate objective—maritime power projection (see figure below)—projecting U.S. power and influence from the sea, directly and decisively influencing events ashore.

Environment control and attack are two ways, both enabled by IO, to attain forward presence and knowledge superiority. Environment control encompasses the range of actions required to assure U.S. access and shape the environment to support the commander. Future Navy forces will continue to face adversaries outside the generally accepted force-on-force environment of the past, as adversaries strive to circumvent or undermine U.S. military strengths and exploit friendly vulnerabilities. Naval forces are challenged by asymmetric operations in all domains —surface, subsurface, air, and cyberspace—and must therefore defend against, defeat, deny, or negate the capabilities that will be used to prevent U.S. freedom of access. Attack exploits the advantages of maneuver and firepower from the sea. The speed of employment afforded by information superiority and networked forces will permit U.S. forces to project power deep inland. Network-centric operations link shooters, sensors, and commanders and permit effects-based planning in order to provide the knowledge required to rapidly attack an adversary's critical vulnerabilities, avoid its strengths, and destroy or shape its center of gravity. Improving the speed and reliability of the information in the local and global information grids ensures that the commander can deliver attacks for desired effects.

Information Superiority

Information superiority, a relative quality not readily measured, embodies the ability to collect, process, and disseminate the correct information to the right person, at the right place and time, in the right form, while denying an adversary the ability to do the same. Adoption of network-centric operations can foster information superiority, but only with high-value information shared in the network. There are five dimensions of information that determine whether or not information is of value to the commander. These are:

- Accuracy - the degree to which the information reflects the actual situation.
- Relevance - the degree to which the information is applicable to the situation.
- Timeliness - the degree to which the information is available in time to affect the decision.
- Usability - the degree to which the information is in a format easily understood by the decision maker.
- Completeness - the degree to which all the information required by the decision maker is available.

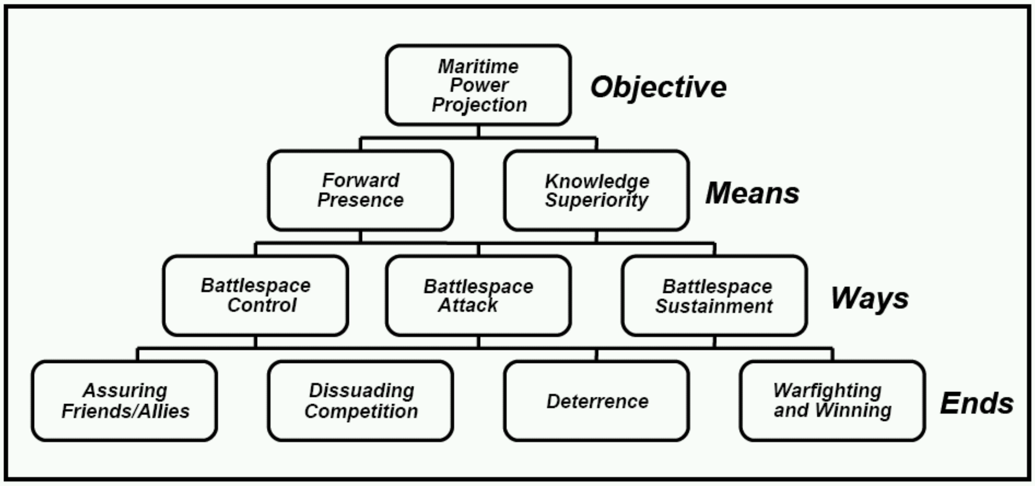


Figure 1. Supporting Maritime Power Projection

IO achieves information superiority by corrupting, deceiving, delaying, denying, disrupting, degrading, or destroying one of the dimensions of information before it is presented to the adversary's commander, while protecting the same friendly information dimensions. This superiority contributes to the ability to project maritime power forward from the sea, and ultimately to have full-spectrum dominance. All echelons strive for and plan to achieve and maintain information superiority. This temporary state may exist in some areas of the environment and not others. It requires a coordinated effort among the operations, intelligence, and command, control, communications, and computers (C4) staffs to achieve information superiority.

Core Capabilities of Information Operations

IO includes actions taken to influence, affect, or defend information, information systems, and decision making. The Chief of Naval Operations (CNO) has established IO as a warfare area within the Navy aimed at protecting and defending our decision-making processes and attacking adversary's decision-making processes by affecting or protecting the accuracy, usability, timeliness, completeness, or relevance of information used by the decision maker in selecting a COA. IO includes EW, Computer Network Operations (CNO), PSYOP, MILDEC, and OPSEC. Supporting capabilities of IO include physical attack, physical security, information assurance, PA, civil-military operations, legal affairs, meteorology, intelligence, cryptology, and oceanography.

IO is an integral part of the Navy planning and targeting process. From guiding effects-based planning in the earliest stages to the weaponeering assessment phase of the targeting cycle, IO planners can assist in determining the right mix of maneuver, and kinetic/nonkinetic weapons that will produce the commander's desired effect. In addition to offering non-kinetic options to traditional strike warfare, IO plans often require the use of strike group maneuver (concentration of forces and presence), kinetic strikes, and special operations warfare to deny, disrupt, destroy, or degrade information systems to attain overall campaign objectives. While each capability of IO includes a specialized planning process and can be applied to military operations individually, their coordinated application maximizes friendly advantages.

Target Set

Warfighters win engagements and wars when the adversary makes a decision—based on knowledge derived from true or perceived information—to surrender, due to an inability to obtain desired objectives. Friendly forces design all campaign plans to influence the adversary to make such a decision. The people and systems that comprise the information grids filter and process the information upon which the commander bases decisions, and therefore require defending as part of IO planning. IO influences the information in the grids to achieve the ultimate goal of influencing the decision maker to behave in a manner that supports the commander's campaign plan. IO plans affect the accuracy, timeliness, relevance, usability, or completeness of information entering the adversary information grids so that the adversary decision maker makes decisions based on information favorable to U.S. desires. Identifying the adversary decision maker through the efforts of the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and operations communities requires a detailed understanding of adversary strengths and weaknesses, organization, doctrine, and decision-making processes.

Environment Awareness and Shaping

EAS describes the functions performed by the IO organization to ensure that, despite the wide range of non-lethal and lethal means at the disposal of adversaries or potential adversaries, friendly forces are consistently capable of conducting decisive operations and achieving desired results at minimal loss to friendly forces. The commander uses EAS to identify, protect, and leverage critical information systems, emissions, transmissions, and operational indicators, to achieve and maintain information superiority.

Environment Awareness

U.S. presence throughout the world makes it imperative that the military, especially forward deployed forces, be keenly aware of the operating environment and IO capabilities of allies and potential adversaries. Today's information-rich and technologically advanced environment has broadened the commander's environment as more information has been made available through the information grids.

Environment awareness results from the continuous process of monitoring IO within an AOR; conducting capability versus vulnerability studies with regard to the operational environment; and reporting on significant events or changes. Environment awareness equates to knowledge of the operational environment. This knowledge, resulting from the fusion of key elements of information, allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish requirements and priorities, and exploit emerging opportunities, while mitigating the impact of unexpected adversary actions.

Network centric operations (NCO) will increase the Navy's overall environment awareness by overcoming the limitations of stand-alone sensors. NCO, enabled through IO, will create a Navy capable of maritime power projection, ensuring access to the littoral areas and deterring conflict through the employment of a network of sensors and communication devices that provide the Navy with real-time, shared awareness in support of operational objectives. NCO enables the force by applying speed in information gathering and sharing, and converting information into knowledge, command, and timely application of effects.

Each echelon of command is responsible for maintaining environment awareness and providing input into ongoing environment-shaping efforts. The higher the echelon of command, the broader the scope of data needed to maintain environment awareness.

Environment Shaping

Environment shaping is the conscious action of molding the environment to prevent conflicts or placing U.S. interests in a favorable position. It provides the foundation of the force commander's message. From a posture of forward presence, the Navy advances national security policy by applying sea power through the fleet or Navy component commander to help shape the international environment via deterrence, peacetime engagement activities, and active participation and leadership in alliances. Environment shaping is the continual process of developing, evaluating, and revising the force operational profile within the environment, providing all warfare commanders with critical planning and execution support to ensure that missions are conducted with the least risk to friendly assets. Environment shaping encompasses all actions taken, including those by PA and CA in both the electronic and physical domains to convey, deny, or protect selected information and images.

Information Operations Organization Structure

- **Naval Network Warfare Command**

  Naval Network Warfare Command (NAVNETWARCOM) provides the Navy's central operational authority and type commander for IO in support of naval forces afloat and ashore. NAVNETWARCOM maintains responsibility for identifying, coordinating, and assessing the Navy's IO requirements and also serves as the operational forces' advocate in the development of IO. As the functional component for IO under USSTRATCOM, NETWARCOM is responsible for the Navy's strategic IO planning and operational support. (Note: Commander Naval Security Group has been formally disestablished as a separate command and now operates as NETWARCOM IO Directorate (IOD).

- **Navy Information Operations Command – Suitland (formerly Naval Information Warfare Activity)**

  The Navy Information Operations Command (NIOC) - Suitland is the Navy's principal technical agent for research and development of prototype IO capabilities. NIOC Suitland supports the development capabilities encompassing all aspects of IO attack, protect, and exploit; maintaining an aggressive program to acquire and analyze state-of-the-art technologies (software and hardware), evaluate fleet applicability, and prototype developmental capabilities. NIOC Suitland is the Navy's interface with other service and national IO organizations that develop IO capabilities. Its activities are closely coordinated with NIOC Norfolk (below) to develop IO technical capabilities for naval and joint operations. NIOC Suitland also supports development coordination between NAVNETWARCOM, , OPNAV, Systems Commands, IO Technology Center, and industry.

- **Navy Computer Incident Response Team**

  The Navy Computer Incident Response Team (NAVCIRT) coordinates the defense of the Navy computer networks from attack, and accomplishes other CND missions as directed by the Commander JTF-GNO and the United States Strategic Command (USSTRATCOM). Naval Network and Space Operations Command (NNSOC) and NIOC Norfolk provide operational support to NAVCIRT, in areas such as the Navy's Computer Network Operations red team

- **Navy Information Operations Command – Norfolk (formally Fleet Information Warfare Center – FIWC)**

  NIOC Norfolk, the Navy's center of excellence for IO, is responsible for providing operationally focused training; planning support and augmentation from the tactical to the strategic level; developing IO doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; and providing and managing IO data for Fleet Operations. ,. NIOC operates under the operational and administrative control of COMNAVNETWARCOM, and has two subordinate commands: NIOC San Diego (formerly FIWC Detachment San Diego and NSGA San Diego) and NIOC Whidbey Island (formerly NSGA Whidbey Island).

Navy Information Operations Employment Concept

Sea Power 21 describes future naval operations that will use information superiority and dispersed, networked force capabilities to deliver effective offensive power, defensive assurance, and operational independence to joint force commanders. To support Sea Power 21, the Navy's focus is to integrate and align IO to support all levels of operations:

- At the strategic level, national leadership and regional commanders will use IO to achieve national/theater shaping and influencing objectives. Regional commanders will integrate Navy IO capabilities with other Services, other U.S. government departments and agencies, and partner nations as part of their Theater Security Cooperation Plans (TSCP). At this level, IO is a key element of effects-based operations.
- At the operational level, IO supports campaign/major operational objectives by providing information superiority through shaping and controlling the information environment. At this level, the focus of IO is control of adversary lines of communication (logistics information, command and control, and related capabilities and activities) while protecting the friendly information environment.
- At the tactical level, Navy IO will make full use of the core capabilities to dominate the information environment for the commander. At this level, IO will be used to tactically influence adversaries; or deny, destroy, or degrade systems critical to the adversary's conduct of operations.

Operational Level	IO is…	IO Objectives	Navy Role	Impact
Strategic (National and Theater)	Key element of national and theater shaping operations	Influence nations/potential adversaries/decision makers globally or in a specific region(s). Support diplomacy, stabilize regions, and assure allies. Deter war. Support intelligence preparation of the environment, and shape environment to U.S. advantage.	Support TSCPs through presence, public affairs, port calls, multinational exercises, peace operations, Navy IO support to strategic communications Guided by the regional combatant commander (RCC) and Navy component commander (NCC).	Demonstrate that the U.S. is engaged in the region and can project power. Demonstrate that the U.S. military can project power anywhere in region. Prepare intelligence baseline for future ops.
Operational	Operations to decisively defeat adversary ability to control forces.	Shape and control information environment. Use spectrum of IO core capabilities to conduct (or support) force application, deny adversary intelligence, surveillance, reconnaissance (ISR) and command, control, communications, computers (C4). Support information superiority. Protect friendly information environment.	Continuing strategic roles plus applying Navy IO capabilities and weapons (OPSEC, CNO, MILDEC, EW) to attack adversary C4 and ISR and PSYOP to influence adversary forces/populations. Directly support conduct of joint or maritime operations/force projection. Guided by NCC or joint force maritime component commander (JFMCC) if a joint task force is established.	Support information superiority for the joint force commander. Control information environment by influencing, disrupting, or corrupting adversarial human and automated decision-making.
Tactical	Navy warfare area - IO warfare commander controlling EW, PSYOP, MILDEC, CNO, OPSEC capabilities embedded in Navy forces.	Control tactical information environment. Disrupt adversary operations. Undermine adversary ability and will to fight. Disrupt adversary C4, ISR and defensive systems. Protect the naval/joint battle force.	During initial phases of a campaign, Navy forces may have the preponderance of tactical IO assets. These capabilities are applied to support commander's objectives, and tactical operations. Guided by strike group commander.	Achieve/maintain decision superiority, control environment, achieves operational objectives of the JFMCC and tactical objectives of the strike group commander.

The following key organizational concepts are being implemented to affect the operational model summarized above:

Joint Force Maritime Component Commander Level – IO Cell [extract from TACMEMO 3-32-03 (JFMCC)]

The JFMCC IO Cell contributes to the shaping of the environment to enable tactical units to successfully execute assigned tasks. To have greatest effect, IO should be initiated well before the start of other operations and continue after decisive operations are concluded. IO actions occur at all levels of government (political strategic, military strategic, operational and tactical) and are a continuous effort. It is vital to the success of IO that JFMCC coordinate planning and execution with other military and government agencies.

The IO cell plans IO actions to achieve JFMCC objectives. JFMCC IO supports JFC and other component efforts with the aid of interoperable collaborative planning tools. One planning tool suite is the Information Warfare Planning Capability (IWPC), which will evolve into IO Planning Capability Joint (IOPC-J).

During mission analysis the status of ongoing IO actions to shape the environment should be briefed to determine if such actions should be intensified or otherwise modified. The inclusion of IO considerations at the start of planning and task development will also influence the targeting process. The IO cell representative should ensure that the objectives are written so as not to specify the method to be used to achieve an objective.

The skill sets required to plan IO are unique and need to be present in the IO cell. As such, the IO cell consists of IO planners, subject matter experts/planners for each IO capability, Special Information Operations planners and intelligence support to include targeteers specific to IO.

The IO Cell coordinates with the other JFMCC staff cells (i.e. horizontally) and with the IO cells of the other components and other government agencies through the JFC IO staff (i.e. vertically). The IO cell works with elements of both the common operational picture (COP) cell and the Future Operations (FUOPS) cell.

The IO cell provides planners to participate in operational planning teams (OPTs) established in the FUOPS cell. They will ensure the IO plan that incorporates the salient details for each applicable IO capability, and is integrated and deconflicted with the overall JFMCC plan. The IO planner will provide guidance to the subject matter experts for each IO capability in the IO cell to develop appropriate actions. The IO planner will integrate these actions into a composite plan and with IO cell director approval represent the IO contribution to the FUOPS OPT as they are formed. Multiple planning efforts/OPTs may occur at the same time in the FUOPS. The IO planner must ensure IO as a contributing part to one planning effort does not conflict with IO portion of another due to the long-term nature of some of the IO actions.

- **Strike Group Level - The IO Warfare Commander (IWC)**

  The IWC is responsible to the force commander for protection of the force against hostile information, information systems, and electronic attacks, as well as hostile propaganda and deceptive techniques. The IWC is also responsible to the force commander for using IO to support all force plans and evolutions; coordinating this effort with theater and joint task force (JTF) IO and IO planners; and disseminating IO surveillance data to the force to ensure an information advantage at critical times in the battle. The IWC establishes and maintains the tactical IO picture through environment awareness and shaping, mission-oriented planning, and execution and monitoring of plans.

  <u>Specific areas of responsibility:</u>

  - The IWC controls force emitters for the OTC/CWC, releasing control of applicable systems through emissions control (EMCON). Additionally, the IWC controls all information and information systems for the force commander, releasing them through information conditions (INFOCON). Therefore, radars, acoustic emitters, information, information systems, and communications are within the IWC's sphere of responsibility. The IWC is responsible for maintaining a favorable tactical situation (TACSIT), and protecting and crafting the desired force operational profile and signature.

  - The IWC directs the employment of numerous SG IO capabilities for the force commander. These capabilities include deception, electronic attack, communications, sensors, combat systems and applications, PSYOP broadcasts, and product dissemination.

  - The IWC is responsible for the core IO staff and the efforts of IO personnel throughout the force who contribute to IO planning and execution.

- **Shore Support - Network Operations, Information Operations, and Space Center**

  COMNAVNETWARCOM has established the Network Operations (NETOPS), IO, and Space Center (NIOSC) as the focal point for providing comprehensive IO support to joint force maritime component commanders (JFMCCs) and strike groups engaged in deliberate/crisis planning and targeting. Watch personnel assigned to the Navy Global Network Operations And Security Center (NAVGNOSC), Navy Computer Incident Response Team (NAVCIRT), Navy Space Operations Command (NAVSOC) and Navy Information Operations Command-Norfolk Maritime Integration Center (MIC) report to the NIOSC to ensure IO is coordinated and integrated across NETWARCOM mission areas.

Supporting Activities

- **Public Affairs**

  PA plays a large role in supporting IO in all operations. A commander can utilize PA to expedite the flow of accurate and timely information to a real or potential adversary. IO coordination with PA may include ensuring critical information protection for a certain period of time in order to minimize the risk to friendly forces, or countering adversary propaganda. PA, CA, and PSYOP may use the same media to communicate similar or, in some cases, identical messages to different audiences. While CA and PSYOP address local populations and adversary forces, PA operations are directed toward U.S. forces, and U.S. and international media. Care must be taken to avoid disseminating contradictory information via the CA, PSYOP, and PA channels.

- **Civil Affairs and Civil Military Operations**

  CA encompasses activities that the military commander employs to establish and maintain relationships with civil authorities, general populations, resources, and institutions in friendly, neutral, or hostile areas. They support the commander's regional strategy and long-term goals by strengthening the capabilities of a host nation (HN) to effectively apply its indigenous resources to mitigate or resolve instability, privation, or unrest. CA and PSYOP are mutually supportive within civil-military operations (CMO). During MOOTW, PSYOP supports various CA activities (e.g., establishes population control measures) to gain support for the HN government in the international community and to reduce support or resources for those destabilizing forces threatening legitimate processes of the HN government. CA personnel and forces can advise commanders on the most effective military efforts to support friendly or HN civilian welfare, security, and developmental programs; PSYOP maximizes these efforts through information products and programs. PSYOP publicizes the existence or successes of these CMO activities to generate target population confidence in, and positive perception of, U.S. and HN actions.

Integrating Information Operations

Escalating to conflict requires rapid transition from daily EAS to detailed, integrated planning with other staff codes, commands, services, and agencies. The IO cell (at JFMCC and strike group levels) needs to quickly define the support available to ensure that the commander can attain the campaign objectives, capitalizing on experience and ongoing shaping efforts. The primary focus of Navy IO planning occurs at the operational level on the JFMCC staff. The primary force for executing the IO plan in daily shaping operations or in conflict occurs at the tactical level under the direction of the Carrier and Expeditionary strike group commanders.

Forward-deployed fleet, and strike group commanders rely on small cadres of IO professionals on their staffs to conduct EAS on a daily basis. IO staffs are augmented with IO planners and operators, provided by the NIOCs. The IO staff operates closely with the operations department for IO execution and consists of the IO officer, and personnel with expertise in the areas of EW, OPSEC, computer network operations, MILDEC planning, PSYOP, targeting, and ELINT analysis.

The IO planning cell at any level — made up of the IO staff, select command representatives, and liaison officers from other commands and agencies—integrates capabilities and related activities within staff sections to ensure that the IO plan supports the commander's overall campaign plan. Effective IO planning, execution, and monitoring require dedicated coordination with PA, CA, intelligence and cryptology, meteorology, oceanography, Judge Advocate General Corps, communications, and combat systems experts. Personnel in these areas provide crucial information to support the development of IO plans and measures of effectiveness.

Contact: POC for updating this information: William Malone william.d.malone@navy.mil.

Last Updated: December 2005.

This Page Intentionally Blank

Return to Contents

Air Force Information Operations Doctrine

Key doctrinal documents:
AFDD 2–5, *Information Operations*, 11 January 2005
AFDD 2–5.1, *Electronic Warfare Operations*, 5 November 2002
AFDD 2–5.3, *Public Affairs Operations*, 24 June 2005

AFDDs are available at: https://www.doctrine.af.mil/ and http://afpubs.hq.af.mil.

Excerpts of Air Force Doctrine - AFDD 2-5

Forward

The Air Force recognizes the importance of gaining a superior information advantage—an advantage obtained through information operations (IO) fully integrated with air and space operations. Today, gaining and maintaining information superiority are critical tasks for commanders and vital elements of fully integrated kinetic and nonkinetic effects-based operations. Information operations are conducted across the range of military operations, from peace to war to reconstitution. To achieve information superiority, our understanding and practice of information operations have undergone a doctrinal evolution that streamlines the focus of IO to improve the focus on warfighting.

The new framework of information operations groups the capabilities of influence operations, electronic warfare operations, and network warfare operations according to effects achieved at the operational level. Each of these capabilities consists of separate and distinct subcapabilities that, when combined and integrated, can achieve effects greater than any single capability. Integrated Control Enablers (ICE) is a new term used to define what was formerly expressed as information-in-warfare, or IIW. As our understanding of IO has advanced we have come see that ICE are not IO, but rather the “gain and exploit” capabilities that are critical to all air, space, and information operations. This new framework reflects the interactive relationship found between the defend/attack and the gain/exploit capabilities in today’s Air Force.

Foundational Doctrine Statements

Foundational doctrine statements are the basic principles and beliefs upon which AFDDs are built.

- Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air and space operations.
- The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.
- The Air Force defines information superiority as the degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.

- Decision superiority is about improving our capability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. Decision superiority is a relationship between adversary and friendly OODA loop processes.
- The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. Effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources.
- Information operations conducted at the operational and tactical levels may be capable of creating effects at the strategic level and may require coordination with other national agencies.
- IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.
- IO applications span the spectrum of warfare with many of the IO capabilities applied outside of traditional conflict. IO may offer the greatest leverage in peace, pre-conflict, transition-to-conflict, and reconstitution.
- Air Force IO may be employed in non-crisis support or military operations other than war (MOOTW) such as humanitarian relief operations (HUMRO), noncombatant evacuation operations (NEO), or counterdrug support missions where Air Force elements are subject to asymmetric threats that could hinder operations or place forces at risk.
- IO presents additional challenges in effects-based planning as there are many variables. Many of these variables have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback.

1. The Nature of Information Operations

General

Information operations (IO) are the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Information operations provide predominantly nonkinetic capabilities to the warfighter. These capabilities can create effects across the entire battlespace and are conducted across the spectrum of conflict from peace to war and back to peace. Information superiority is a degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. Information superiority is a critical part of air and space superiority, which gives the commander freedom from attack, freedom to maneuver, and freedom to attack. Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air and space operations. IO, therefore, must be integrated into air and space component operations in the same manner as traditional air and space capabilities.

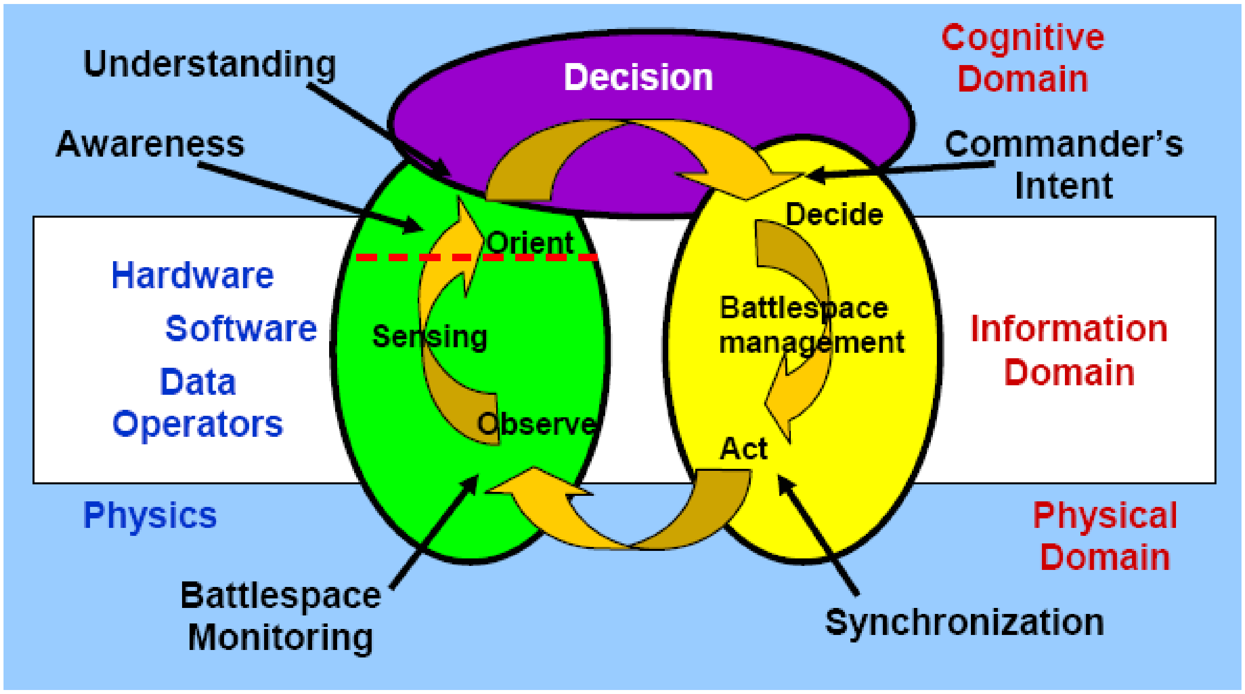
Warfare in the Information Age

Warfare in the information age has placed greater emphasis on influencing political and military leaders, as well as populations, to resolve conflict. Information technology (IT) has increased access to the means to directly influence the populations and its leaders. IT has distributed the process of collection, storage, dissemination, and processing of information. The Air Force goal is to leverage this technology to achieve air, space, and information superiority and to be able to operate in a faster decision cycle (decision superiority) than the adversary. Decision superiority is a competitive advantage, enabled by an ongoing situational awareness, that allows commanders and their forces to make better-informed decisions and implement them faster than their adversaries can react. Decision superiority is about improving our ability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. *Joint*

Vision 2020 describes it as “better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.” Decision superiority is a relationship between adversary and friendly OODA loop processes. Decision superiority is more likely to be achieved if we plan and protect our OODA loop processes in conjunction with analyzing, influencing, and attacking the adversary’s.

The Information Environment

[The information environment can be modeled as the interaction of the physical, information, and cognitive domains as shown below.]



This model provides a means to understand the IO environment. It also provides a logical foundation for the IO capabilities of influence operations, network warfare operations, and electronic warfare operations. All activities in the physical environment have effects in the cognitive environment. Electronic warfare operates in the electromagnetic spectrum, although it creates effects across the range of the IO operating environment. Network warfare operations are focused on the information domain, which is composed of a dynamic combination of hardware, software, data, and human components. Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. The means of influencing can be physical, informational, or both. The cognitive domain is composed of separate minds and personalities and is influenced by societal norms, thus the cognitive domain is neither homogeneous nor continuous.

Societies and militaries are striving to network this “information domain” with the objective of shortening the time it takes for this distributed observe, orient, decide, and act process to occur. It also allows us to automate certain decision processes and to build multiple decision models operating simultaneously. In essence, the information domain continues to expand. New technology increases our society’s ability to transfer information as well as an adversary’s opportunity to affect that information. Information operations are not focused on making decision loops work; IO focuses on defending our decision loops and influencing or affecting the adversary’s decisions loops. This integration of influence, network warfare, and electronic warfare operations to create effects on OODA loops is the unifying theme of IO. Whether the target is national leadership, military C2, or an automated industrial process, how the OODA process is implemented provides both opportunities and vulnerabilities.

Return to Contents

The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. In addition, effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources. The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.

Influence Operations

Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives. The military capabilities of influence operations are psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, counterpropaganda operations and public affairs (PA) operations. Public affairs, while a component of influence operations, is predicated on its ability to project truthful information to a variety of audiences.

Network Warfare Operations

Network warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Networks in this context are defined as any collection of systems transmitting information. Examples include, but are not limited to, radio nets, satellite links, tactical digital information links (TADIL), telemetry, digital track files, telecommunications, and wireless communications networks and systems. The operational activities of network warfare operations are network attack (NetA), network defense (NetD) and network warfare support (NS).

Electronic Warfare Operations

Electronic warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. Electronic warfare operates across the electromagnetic spectrum, including radio, visible, infrared, microwave, directed energy, and all other frequencies. It is responsible for coordination and deconfliction of all friendly uses of the spectrum (air, land, sea, and space) as well as attacking and denying enemy uses. For this reason it is a historically important coordinating element in all operations, especially as current and future friendly uses of the electromagnetic spectrum multiply. The military capabilities of electronic warfare operations are electronic attack, electronic protection, and electronic warfare support.

Integrated Control Enablers

Information operations, like air and space operations, are reliant on the integrated control enablers (ICE). ICE includes intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT). Information operations are highly dynamic and maneuverable. The transition between the find, fix, track, target, engage, and assess (F2T2EA) phases can be nearly instantaneous. The ICE components support this interactive relationship and strive to provide commanders continuous decision-quality information to successfully employ information operations.

2 – Influence Operations

General

Influence operations are employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives. They should influence adversary decision-making, communicate the military perspective, manage perceptions, and promote behaviors conducive to friendly objectives. Counterpropaganda operations, psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, and public affairs (PA) operations are the military capabilities of influence operations. They support the commander's objectives and support the Air Force in achieving air, space, and information superiority. This is accomplished by conveying selected information and indicators to target audiences; shaping the perceptions of target decision-makers; securing critical friendly information; protecting against espionage, sabotage, and other intelligence gathering activities; and communicating unclassified information about friendly activities to the global audience.

Psychological Operations

Focused on the cognitive domain of the battlespace, PSYOP targets the mind of the adversary. In general, PSYOP seeks to induce, influence, or reinforce the perceptions, attitudes, reasoning, and behavior of foreign leaders, groups, and organizations in a manner favorable to friendly national and military objectives. PSYOP supports these objectives through the calculated use of air, space, and IO with special emphasis on psychological effects-based targeting.

Military Deception

Military deception (MILDEC) capabilities are a powerful tool in military operations and should be considered throughout the operational planning process. Military deception misleads or manages the perception of adversaries, causing them to act in accordance with friendly objectives.

Operations Security

Operations security (OPSEC) is an activity that helps prevent our adversaries from gaining and exploiting critical information. OPSEC is not a collection of specific rules and instructions that can be applied to every operation, it is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the adversary. Critical information consists of information and indicators that are sensitive, but unclassified. OPSEC aims to identify any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities.

Counterintelligence

The Air Force Office of Special Investigations (AFOSI) initiates, conducts, and/or oversees all Air Force counterintelligence (CI) investigations, activities, operations, collections, and other related CI capabilities. Counterintelligence is defined as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. AFOSI supports influence operations through CI operations designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, manipulation, deception, or repression of the adversary.

Public Affairs Operations

Commanders conduct PA operations to assess the information environment in areas such as public opinion and to recognize political, social, and cultural shifts. Public affairs operations are a key component of informational flexible deterrent options and build commanders' predictive awareness of the international public information environment and the means to use information to take offensive and preemptive defensive actions in Air Force operations. Public affairs operations are the lead activity and the first line of defense against adversary propaganda and disinformation. Falsehoods are easily identified when the truth is well known. [Public affairs operations are accomplished through] four core tasks: media operations, internal information, community relations, and strategic communication planning.

Counterpropaganda Operations

The Air Force defines counterpropaganda operations as activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations and military forces situational understanding. They involve those efforts to negate, neutralize, diminish the effects of, or gain an advantage from foreign psychological operations or propaganda efforts.

Supporting Activities

Influence operations are most successful through the seamless integration of kinetic and nonkinetic capabilities. Influence operations may be supported and enhanced by physical attack to create or alter adversary perceptions. Influence operations require support from many Air Force capabilities to include tailored ISR, combat camera operations, and cultural expertise.

3 – Network Warfare Operations

Network warfare operations (NW Ops) are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NS). The integrated planning and employment of network warfare operations along with electronic warfare operations (EW Ops), influence operations, and other military capabilities are conducted to achieve desired effects across the information domain.

Network Attack

Network attack (NetA) is employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. Additionally, NetA can be used to deny, delay, or degrade information resident in networks, processes dependent on those networks, or the networks themselves. A primary effect is to influence the adversary commander's decisions.

Network Defense

Network defense (NetD) is employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it. NetD can be viewed as planning, directing, and executing actions to prevent unauthorized activity in defense of Air Force information systems and networks and for planning, directing, and executing responses to recover from unauthorized activity should it occur.

Network Warfare Support

Network warfare support (NS) is the collection and production of network related data for immediate decisions involving NW Ops. NS is critical to NetA and NetD actions to find, fix, track, and assess both adversaries and friendly sources of access and vulnerability for the purpose of immediate defense, threat prediction and recognition, targeting, access and technique development, planning, and execution in NW Ops.

4 – Electronic Warfare Operations

General

Electronic warfare (EW) is any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack an adversary. The Air Force describes electronic warfare operations (EW Ops) as the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. The EW spectrum is not merely limited to radio frequencies but also includes optical and infrared regions as well. EW assists air and space forces to gain access and operate without prohibitive interference from adversary systems, and actively destroys, degrades, or denies opponents' capabilities, which would otherwise grant them operational benefits from the use of the electromagnetic spectrum.

Electronic Warfare Operations

EW is a key contributor to air superiority, space superiority, and information superiority. The most important aspect of the relationship of EW to air, space, and information operations is that EW enhances and supports all operations throughout the full spectrum of conflict. Air Force EW resources and assets may take on new roles in support of operations as the electronic warfare operation mission evolves. The three military capabilities of EW operations are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). All three contribute to air and space operations, including the integrated IO effort. Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems.

Electronic attack (EA) is the division involving the use of electromagnetic, directed energy (DE), or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of deceiving, disrupting, denying, and/or destroying adversary combat capability. It also deceives and disrupts the enemy integrated air defense system (IADS) and communications, as well as enables the destruction of these adversary capabilities via lethal strike assets.

Electronic protection (EP) enhances the use of the electronic spectrum for friendly forces. Electronic protection is primarily the defensive aspect of EW that is focused on protecting personnel, facilities, and equipment from any effects of friendly or adversary employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

Electronic warfare support (ES), the collection of electromagnetic data for immediate tactical applications (e.g., threat avoidance, route selection, targeting, or homing) provides information required for timely decisions involving electronic warfare operations.

5 – Information Operations Planning and Execution

Information operations are integral to military operations and are a prerequisite for information superiority. IO supports, and may also be supported by, air and space operations and needs to be planned and executed just like air operations. IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.

One of the commander's priorities is to achieve decision superiority over an adversary by gaining information superiority and controlling the information environment. This goal does not in any way diminish the commander's need to achieve air and space superiority but rather facilitates efforts in those areas and vice versa. The aim of information superiority is to have greater situational awareness and control than the adversary. Effective use of IO leads to information superiority. The effort to achieve information superiority depends upon two fundamental components: an effects-based approach, and well-integrated IO planning and execution accomplished by IO organizations.

Effects-Based Approach

The ability to create the effects necessary to achieve campaign objectives, whether at the strategic, operational, or tactical levels, is fundamental to the success of the Air Force. An effect is the anticipated outcome or consequence that results from a particular military operation. The emphasis on effects is as crucial for successful IO as for any other air and space power function. Commanders should clearly articulate the objectives or goals of a given military operation. Effects should then flow from objectives as a product of the military operations designed to help achieve those objectives. Based on clear objectives, planners should design specific operations to achieve a desired outcome, and then identify the optimum capability for achieving that outcome. It is important to realize that operational assessment may be more challenging in IO because the effects are often difficult to measure. IO may also be based upon common sense, a rule of thumb, simplification, or an educated guess that reduces or limits the search for solutions in domains that are difficult or poorly understood. For example, psychological effects are not only difficult to measure; they may also not manifest themselves until later in time. There are also second-order and third-order effects that should be taken into consideration, and again, these may not manifest themselves until much later. IO presents additional challenges in effects-based planning as there are many variables. Many of these variables also have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback. At all times, objectives must be set and effects must be analyzed from the point of view of the culture where operations are being conducted.

Information Operations Organzations

A number of Air Force organizations contribute to effective IO. The following discuss several of the key organizations employed in information operations.

Information Warfare Flight (IWF)

IO can be conducted throughout the spectrum of peace and conflict. In peacetime, the major command/ numbered air force (MAJCOM/NAF) IWF is the operational planning element for IO and may coordinate IO actions when an air and space operations center (AOC) has not been activated. When the AOC is activated, a portion of the IWF is established as an IO team and integrates into the warfighting divisions within the AOC (Strategy, Plans, ISR, Combat Operations, etc.). The IO team provides the IO expertise to plan, employ, and assess IO capabilities prior to the initiation of hostilities, transition to conflict, and reconstitution.

EW Ops Organizations

Electronic warfare is conducted by units with capabilities ranging across the electronic attack, protect, and support functions. EW operations require attention before, during, and after military operations. A joint EW coordination cell (EWCC) is the necessary planning and execution organization to orchestrate the activities of units to achieve EW objectives of the campaign plan.

Network Defense and Network Operations Organizations

NetD and NetOps organizations provide the JFC with critical capabilities to realize the effects of information and decision superiority. Collectively, these organizations provide varying degrees of NetD and NetOps support. They provide commanders with real-time intrusion detection and perimeter defense capabilities, network management and fault resolution activities, data fusion, assessment, and decisions support. During employment, the organizations are arranged into a three-tiered operational hierarchy, which facilitates synchronized application of their collective capabilities in support of the DOD's defense-in-depth security strategy.

6 – Integrated Control Enablers

Information operations are dependent on [integrated control enablers] (ICE). The integrated control enablers are critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. These include intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT).

Network Operations and Information Assurance

NetOps encompasses information assurance (IA), system and network management, and information dissemination management. The Air Force and joint community have come to recognize these pillars as information assurance and network defense, enterprise service management/network management, and content staging/information dissemination management respectively. NetOps consists of organizations, procedures, and functionalities required to plan, administer, and monitor Air Force networks in support of operations and also to respond to threats, outages, and other operational impacts.

Information assurance (IA) comprises those measures taken to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation (ability to prove sender's identity and prove delivery to recipient). IA spans the full lifecycle of information and information systems. IA depends on the continuous integration of trained personnel, operational and technical capabilities, and necessary policies and procedures to guarantee continuous and dependable information, while providing the means to efficiently reconstitute these vital services following disruptions of any kind, whether from an attack, natural disaster, equipment failure, or operator error. In an assured information environment, warfighters can leverage the power of the information age.

Intelligence, Surveillance, and Reconnaissance

ISR is the integrated capabilities to task, collect, process, exploit, and disseminate accurate and timely intelligence information. ISR is a critical function that helps provide the commander the situational and battlespace awareness necessary to successfully plan and conduct operations. Commanders use the intelligence information derived from ISR assets to maximize their own forces' effectiveness by optimizing friendly force strengths, exploiting adversary weaknesses, and countering adversary strengths.

Predictive Battlespace Awareness

Effective IO depends upon a successful PBA. As a maturing concept, PBA is "knowledge of the operational environment that allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions" (Air Force Pamphlet 14-118). In order to accomplish this, PBA lays out a methodology that enables integration of all intelligence, surveillance, and reconnaissance assets available to commanders, in order to maximize their ability to predict enemy courses of action and decide friendly courses of action. One of the first steps in PBA is assessing friendly vulnerabilities and adversary strengths and weaknesses in order to predict enemy courses of action through IPB. This level of awareness requires development and integration of five key activities: IPB, target development, ISR strategy and planning, ISR employment, and assessment. These activities are continuously refined in parallel to provide a seamless understanding of the battlespace.

Return to Contents

Precision Navigation and Timing

Precision navigation and timing (PNT) provided by space-based systems are essential to IO by providing the ability to integrate and coordinate IO force application to create effects across the battlespace.

7 – Education and Training

Education and training provide the foundation for conducting effective information operations. All Airmen should have a general understanding of information operations capabilities. As in other specialties, IO personnel should be thoroughly trained in the specific IO processes that relate to their particular field of expertise. IO personnel should recognize the contribution their functional specialty makes to the warfighter to help achieve the goal of information superiority. The intent of IO education and training is to ensure Air Force IO operators clearly understand the principles, concepts, and characteristics of information operations. Finally, while not every Airman needs a comprehensive course in information operations, every Airman should understand that IO is a key function of the Air Force distinctive capabilities of information superiority and air and space superiority.

Note: End of AFDD 2-5 extract.

Air Force Information Operations Organizational Structure

National Air Intelligence Center: National Air Intelligence Center, with headquarters at Wright-Patterson AFB, Ohio, is the primary Department of Defense producer of foreign aerospace intelligence. NAIC develops its products by analyzing all available data on foreign aerospace forces and weapons systems to determine performance characteristics, capabilities, vulnerabilities, and intentions. Center assessments are also an important factor in shaping national security and defense policies. As the DoD experts on foreign aerospace system capabilities, personnel historically have also been involved in supporting American weapons treaty negotiations and verification.

The Air Force Systems Command's Foreign Technology Division was the organizational beginning of today's National Air Intelligence Center. Since the start of its organizational lineage in 1961, the unit's mission and resources have expanded to meet the challenge of worldwide technological developments and the accompanying national need for aerospace intelligence. In recent years, the emphasis has increasingly shifted toward evaluation of worldwide aerospace systems and the production of "tailored," customer-specific products.

AF Air Intelligence Agency with headquarters at Lackland Air Force Base, Texas, realigned under Air Combat Command and Eighth Air Force, serves as their primary information operations force provider normalizing and synchronizing IO capabilities into the warfighter's arsenal.

The AF Air Intelligence Agency's mission is to gain, exploit, defend and attack information to ensure superiority in the air, space and information domains. The agency's people worldwide deliver flexible collection, tailored air and space intelligence, weapons monitoring and information warfare products and services.

With the realignment, the AIA commander serves as the Eighth Air Force deputy commander for information operations. The Eighth Air Force with its bomber and information operations capabilities is the Air Force's first operational force designed to achieve and maintain information superiority. The AIA commander also serves as commander of the Joint Information Operations Center, a subordinate unit of U.S. Strategic Command. The agency has approximately 13,000 people stationed worldwide.

Last Updated: January 2006

DoD and Joint Information Operations Organizations

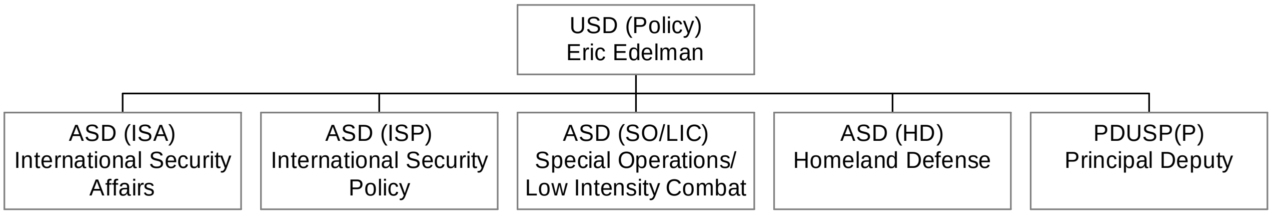
This Page Intentionally Blank

Return to Contents

Under Secretary Of Defense – Policy (USD(P))

Mission

The USD(P) is the principal staff assistant and advisor to the SecDef for all matters concerning the formation of national security and defense policy and the integration and oversight of DoD policy and plans to achieve national security objectives. The USD(P) oversight and policy responsibilities include the IO core capability of PSYOP, and the related capability of Civil Military Affairs, both of which fall within the oversight responsibilities of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SO/LIC)). The Office of the USD(P) is organized as follows:


USD (Policy)
Eric Edelman

ASD (ISA)
International Security Affairs

ASD (ISP)
International Security Policy

ASD (SO/LIC)
Special Operations/ Low Intensity Combat

ASD (HD)
Homeland Defense

PDUSP(P)
Principal Deputy

The directed responsibilities of the USD(P) include the following:

- Represent the Department of Defense, as directed, in matters involving the National Security Council (NSC); the Department of State; and the other Federal Departments, Agencies, and inter-Agency groups with responsibility for national security policy.

- Serve as a member of the NSC Deputies Committee; serve as a member of the Deputies Committee for Crisis Management; and advise the Secretary of Defense on crisis prevention and management, including contingency planning for major areas of concern.

- Develop DoD policy guidance, provide overall supervision, and provide oversight of planning, programming, budgeting, and execution of special operations activities, including civil affairs and psychological operations, and of low-intensity conflict activities, including counter-terrorism, support to insurgency, and contingency operations.

- Develop DoD policy and provide oversight for emergency planning and preparedness, crisis management, defense mobilization in emergency situations, military support to civil authorities, civil defense, and continuity of operations and government.

- Develop policy, coordinate and oversee DoD participation in, and provide staff supervision over special and sensitive activities including the Operations and Support Special Access Program Central Office, and support to the Special Access Program Oversight Committee structure and arms control countermeasures for non-proliferation initiatives; and oversight of the Defense Sensitive Support program.

The Assistant Secretary of Defense for Special Operations/Low Intensity Conflict – ASD(SO/LIC). This office has overall responsibility for the supervision of Special Operations (SO) and Low-intensity Conflict (LIC) activities of DoD - including oversight of policy and resources. The ASD(SO/LIC) is the principal civilian advisor to SECDEF on SO/LIC matters.

The Cohen-Nunn Amendment to the DoD Authorization Act of 1987, established the Office of the ASD(SO/LIC) and the United States Special Operations Command (USSOCOM). The objectives of this amendment were:

- Provide close civilian oversight for special operations and low-intensity conflict activities.
- Ensure that genuine expertise and a diversity of views are available to the President and Secretary of Defense regarding possible responses to special operations requirements and low-intensity conflict threats.
- Improve interagency planning and coordination for special operations and low-intensity conflict.
- Bolster U.S. special operations capabilities in a number of areas to include joint doctrine and training, intelligence support, command and control, budgetary authority, personnel management, and mission planning.

Assistant Secretary of Defense for Homeland Defense – ASD(HD). Authorized by Congress as part of the FY 2003 Defense Authorization Act, the ASD(HD) has overall supervision of the homeland defense activities of the Department. On September 3 2003, DoD realigned Critical Infrastructure Protection oversight from the Undersecretary of Defense (Intelligence) to ASD (HD).

- Supervise the Homeland Defense activities of DOD.
- Develop Homeland Defense force employment policy and guidance.
- Serve as principal point of contact for Department of Homeland Security.
- Develop plans and policy to fulfill DOD's role in Homeland Security.
- Assist in building and improving Federal, State and local homeland security response capabilities.
- Supervise DoD preparedness activities for, and support to, civil authorities.
- Plan, train and perform DoD domestic incident management.
- Advocate Homeland Defense requirements within the Department's resource allocation process.

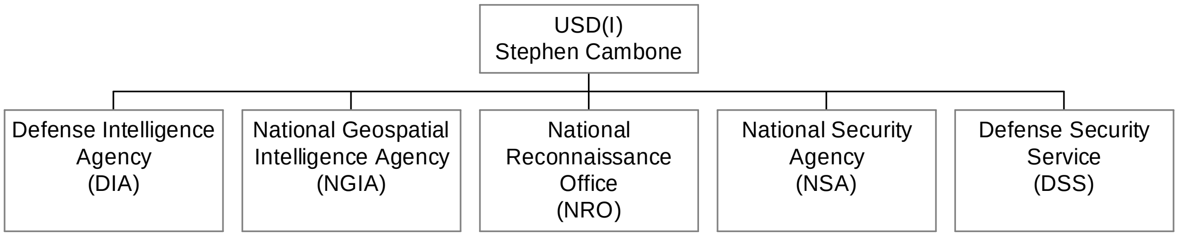
Website: http://www.defenselink.mil/policy/

Last Updated: December 2005

Under Secretary Of Defense –Intelligence (USD(I))

Mission

The Under Secretary of Defense for Intelligence (USD(l)) serves as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense on all intelligence, counterintelligence and security, and other intelligence-related matters. The USD(I) also serves as the PSA to the Secretary of Defense on development and oversight of DoD IO policy and integration issues, and serves as the DoD lead with the Intelligence Community on DoD IO issues.



USD(I)
Stephen Cambone

Defense Intelligence Agency (DIA)

National Geospatial Intelligence Agency (NGIA)

National Reconnaissance Office (NRO)

National Security Agency (NSA)

Defense Security Service (DSS)

Responsibilities:

Information Operations Responsibilities (extracted from DoDD 5143.01, 23 Nov 05)**:**

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DoD IO policy and integration activities.
- Assess performance/responsiveness of DoD and Military Intelligence activities to support IO.
- Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.

Other Responsibilities:

- Service as the OSD proponent for the Information Operations Career Force (See DoDD 3608.11, "Information Operations Career Force", 4 Nov 05).
- Providing oversight and policy guidance for all DoD intelligence activities and establishing priorities to ensure conformance with Secretary and, as appropriate, Director of Central Intelligence (DCI) policy guidance.

- Exercise authority, direction, and control over the Defense Intelligence Agency (DIA), the National Geospatial Intelligence Agency (NGIA), the National Reconnaissance Organization (NRO), the National Security Agency (NSA), the Defense Security Service (DSS), and the DoD Counterintelligence Field Activity (CIFA).

- Provide assessments of and advising the Secretary and the CJCS on the adequacy of military intelligence performance.

- Advise the Secretary concerning the Department's responsibilities regarding the national intelligence community and supporting the Secretary's role in the Intelligence Community Executive Committee.

- Exercise management and oversight of all DoD counterintelligence and security activities, including personnel security and industrial security.

- Oversee intelligence support to critical infrastructure protection, departmental information assurance programs and homeland defense.

- Coordinating DoD intelligence and intelligence-related policy, plans, programs, requirements and resource allocations. This includes responsibility for the DoD components within the National Foreign Intelligence Program, the Joint Military Intelligence Program, the Foreign Counterintelligence Program, and the Tactical Intelligence and Related Activities account.

- Ensuring the execution of DoD intelligence policy and resource decisions are fully responsive and complimentary to the direction of the DCI.

- Exercising overall supervision and policy oversight of the DoD intelligence infrastructure and civilian intelligence personnel management systems. This will include policy regarding the Defense Civilian Intelligence Personnel Systems (DClPS).

- Maintain close coordination with the DCI and consult with the DCI on the development, design, acquisition and operation of intelligence programs and systems of the DOD.

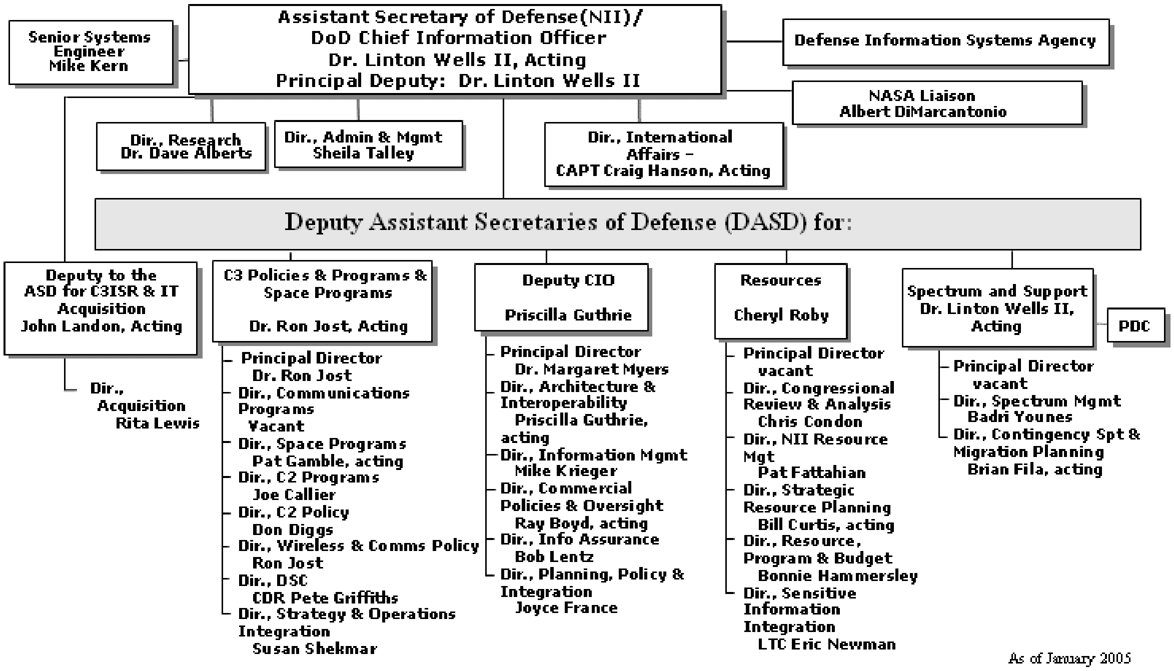
Last Updated: December 2005.

Assistant Secretary Of Defense – Networks And Information Integration (ASD(NII))

Mission and Goals.

The missions and responsibilities of the ASD(NII) are specified in Department of Defense Directive (DoDD) 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO) " dated 2 May 2005.

Organization:


Assistant Secretary of Defense(NII)/
DoD Chief Information Officer
Dr. Linton Wells II, Acting
Principal Deputy: Dr. Linton Wells II
Senior Systems Engineer Mike Kern
Defense Information Systems Agency
NASA Liaison Albert DiMarcantonio
Dir., Research Dr. Dave Alberts
Dir., Admin & Mgmt Sheila Talley
Dir., International Affairs – CAPT Craig Hanson, Acting
Deputy Assistant Secretaries of Defense (DASD) for:
Deputy to the ASD for C3ISR & IT Acquisition John Landon, Acting
Dir., Acquisition Rita Lewis
C3 Policies & Programs & Space Programs Dr. Ron Jost, Acting
Principal Director Dr. Ron Jost
Dir., Communications Programs Vacant
Dir., Space Programs Pat Gamble, acting
Dir., C2 Programs Joe Callier
Dir., C2 Policy Don Diggs
Dir., Wireless & Comms Policy Ron Jost
Dir., DSC CDR Pete Griffiths
Dir., Strategy & Operations Integration Susan Shekmar
Deputy CIO Priscilla Guthrie
Principal Director Dr. Margaret Myers
Dir., Architecture & Interoperability Priscilla Guthrie, acting
Dir., Information Mgmt Mike Krieger
Dir., Commercial Policies & Oversight Ray Boyd, acting
Dir., Info Assurance Bob Lentz
Dir., Planning, Policy & Integration Joyce France
Resources Cheryl Roby
Principal Director vacant
Dir., Congressional Review & Analysis Chris Condon
Dir., NII Resource Mgt Pat Fattahian
Dir., Strategic Resource Planning Bill Curtis, acting
Dir., Resource, Program & Budget Bonnie Hammersley
Dir., Sensitive Information Integration LTC Eric Newman
Spectrum and Support Dr. Linton Wells II, Acting
PDC
Principal Director vacant
Dir., Spectrum Mgmt Badri Younes
Dir., Contingency Spt & Migration Planning Brian Fila, acting
As of January 2005

The goals of ASD(NII) are to:

- Make information available on a network that people depend on and trust
- Populate the network with new, dynamic sources of information to defeat the enemy
- Deny the enemy information advantages and exploit weakness to support network centric warfare and the transformation of DoD business processes

Mission: The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology (IT), including National Security Systems (NSS); information resources management (IRM); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters.

ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the Department. The ASD(NII)/DoD CIO also serves as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective.

Responsibilities of the ASD(NII)/DoD CIO include the following:

- Information Operations: Provide NII and CIO support to the mission of Information Operations IAW DoD Directive S-3600.1.
- Information Assurance: Develop and maintain the DoD Information Assurance (IA) program and associated policies, procedures, and standards required by DoD Directive S-3600.1, "Information Operations ".
- Transformation: Develop and implement network-centric policies, architectures, practices, and processes with emphasis on communications and information networks to enable Defense transformation; however, these do not include content-based communications functions such as those associated with public affairs and public diplomacy.
- Global Information Grid: Facilitate and resolve interoperability, performance, and other issues related to interfaces, security, standards, and protocols critical to the end-to-end operation of the Global Information Grid (GIG).
- IT Opportunities: Identify opportunities presented by communication and information technologies as well as risks and costs, and make recommendations on the initiation of communication and information plans, programs, policies, and procedures accordingly.
- Electromagnetic Spectrum: Provide policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum, including the management and use of the electromagnetic spectrum (MUES) and the Electromagnetic Environmental Effects (E3) Program.
- Command and Control: Develop and integrate the Department's overall C2 strategy, approach, structure, and policies and ensure the C2 structure and architecture are compliant with DoD network-centric precepts, information strategy, and joint needs.
- Space: Oversee DoD non-intelligence related space matters, including space-based communications programs, space-based information integration activities, space control activities, operationally responsive space programs, space access, satellite control, space-based position, navigation, and timing programs, environmental sensing, and space launch ranges.

Headquarters: The headquarters for the ASD(NII) organization is in the Pentagon, with staff elements both in the Pentagon and in nearby office buildings in Arlington, Virginia.

Website: http://www.defenselink.mil/nii/

Last Updated: December 2005

Defense Information Systems Agency (DISA)

Mission:

The Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war.

History of DISA

The Defense Information Systems Agency (DISA) was established as the Defense Communications Agency (DCA) in 1960. Its mission was to manage the Defense Communications System (DCS), a consolidation of the independent long-haul communications functions of the Army, Navy, and Air Force. Later, took on several major organizations, to include the White House Signal Agency (now the White House Communications Agency). DCA also established six regional communications control centers and two area centers for operational control of the DCS. DCA later became responsible for engineering and operating the Worldwide Military Command and Control System.

In the 1980s, DCA absorbed the Joint Tactical Command, Control, and Communications Agency and was renamed DISA in 1991. DCA implemented creation of the Defense Information Infrastructure, now known as the Global Information Grid (GIG). DISA consolidated several information processing centers into five mainframe-processing centers. The Joint Spectrum Center and the Defense Technical Information Center also became part of DISA. Approximately 7,000 military and civilian employees work in DISA.

Core Mission Areas

Communications

DISA provides global classified and unclassified voice, data, video, and transport services through a combination of terrestrial and satellite assets. These assets are dominantly commercial, though acquired and supplemented with military value-added features.

The vast majority of DOD's command and control traffic, voice conferencing, intelligence dissemination, and combat support traffic ride over the joint networks provided by DISA. The aggregate of these networks is referred to as the Defense Information System Network (DISN), which is the key wide-area communications component of the Global Information Grid. Specific subsystems include the Defense Red Switch Network for classified voice conferencing, the Secret Internet Protocol Router Network (SIPRNET), the Non-Secure Internet Protocol Router Network (NIPRNET), Enhanced Mobile Satellite Services (EMSS), the DISN Video Secure Global (DVSG), the Defense Satellite Communications System (DSCS), and the Defense Switched Network (DSN-voice traffic). Underpinning the DISN is a Global Network Operations and Security Control (GNOSC) System to ensure sustained and responsive integrated network operations. In addition, DISA provides tailored Community of Interest Networks (COINs) for specific functional communities that accrue the economic advantage of shared transport and the operational advantages of enhanced security and interoperability with the larger enterprise. All of the above rely on DISA's Global and Regional Network Operations and Security Centers (G/RNOSCs) to perform essential GIG network operations (NETOPS) which is constantly in operation.

Information Assurance

The Quadrennial Defense Review (QDR) recognized Information Operations as a core competency for DoD: "Assuring information systems in the face of attack and conducting effective information operations" is one of the six QDR operational goals. DISA strongly supports these thrusts in its core program. Its information assurance program is broadly focused on designing and deploying proactive protections, deploying attack detection, and on performing information assurance (IA) operations. It secures DoD enterprise systems and provides support to the Combatant Commanders and deployed forces. It also provides capstone capabilities for the entire department such as the DoD Computer Emergency Response Team (CERT), the DOD-wide anti-virus license, the DoD Public Key Infrastructure (PKI), and accreditation and certification process, policy, and implementation. DISA also has a core responsibility as the C3 Critical Infrastructure Protection (CIP) defense sector lead component.

Cyber attacks happen very quickly and often with great stealth. Critical warfighting processes must continue to function effectively while under cyber attack. The DISA information assurance strategy is based on the idea that appropriate defenses must stop most attacks. Protection mechanisms include the following constituents:

- Physical Component
- Electronic Component
- Procedural Component.

The defenses must then be kept current during rapid evolutions of technology, attack strategies, and organizational change; this takes a significant technical and operational effort. Should an adversary breach these protections, DoD must have the capability to detect, contain, and then respond to an attack. DISA's efforts include:

- Hardening of joint enterprise communications, command and control, computing, and messaging to include perimeter defenses, critical infrastructure protection, and security for specific high-value joint systems to include the:
    - Defense Information Systems Network.
    - Global Command and Control System.
    - Combat Support Computing in the Defense Enterprise Computing Centers.
    - Defense Message System.
- Providing the DoD Computer Emergency Response Team (CERT) and, through it and the Global Network Operations and Security Center (GNOSC), providing primary support to the Joint Task Force-Global Network Operations (JTF-GNO).
- Deploying, operating, and monitoring defenses and a sensor grid at key locations, and at gateways between DoD and others.
- Developing, deploying, and operating tools to enable coordination of attack analysis and attack response across various DoD operational entities.
- Providing direct assistance to Combatant Commanders for information assurance to include technical protection, assistance visits, and operational support.

- Development and implementation of a DOD-wide vulnerability management program, a Defense Information Technology Security Certification and Accreditation process (DITSCAP), and secure configuration standards.

- Developing, deploying, and operating the single DoD cyber identity credential infrastructure, the DoD public key infrastructure (PKI) and a secure global directory service.

- Developing and deploying tools and security designs to enable coalition operations.

- Providing site licenses for key joint information assurance tools and DOD-wide product licenses for anti-virus software.

- Providing a deployable Joint Spectrum Interference Resolution (JSIR) Team, which provides primary engineering support to identify, track, and mitigate interference and electronic attacks against DoD systems.

During the 2002 calendar year, GNOSC, DoD CERT, and JTF-GNO detected, analyzed, and responded to more than 46,000 "events" on DOD's unclassified networks. In one example, gateway ports were blocked within two hours of the first reports of the Microsoft Structured Query Language (SQL) "Slammer" worm, effectively preventing further compromise of DoD systems from the Internet. They also deployed signatures on intrusion detection devices to alert network security managers across the globe of any Slammer-related activity. As a result, there were only 264 confirmed infections throughout DOD's 14,774

Combat Support Computing

DISA provides mainframe and server computer operations, production support, technical services and end user assistance for command and control, combat support, and eBusiness functions across DOD. DISA's has five Defense Enterprise Computing Centers (DECCs) and their detachments. As an integral component of the Global Information Grid (GIG), DISA's combat support computing provides global reachback, end-to-end control, defensive information operations, and operational sensitivity. Further, the DISA-fielded Global Combat Support System (GCSS) provides commanders with web-based access to selected Service and Agency authoritative/preferred logistics and transportation databases.

Command and control applications are developed by Services' and Agencies' central design activities. Despite the lack of development standards and the disparate, stovepiped nature of the applications, DISA provides common computing platforms, networks, and enterprise systems management tools that serve to standardize the underlying infrastructure and integrate the combat support business processes it supports. Using the global reachback provided by DISN, a joint task force can plug into this common computing infrastructure to get full, interoperable support. Through the Global Command and Control System (GCCS), and a common communications and computing infrastructure, DISA provides the joint warfighter with a single, end-to-end capability to manage and monitor units, personnel, and equipment from mobilization through deployment, employment, sustainment, redeployment, and demobilization.

Joint Command and Control

DISA is the single DoD integrator for joint, coalition, and combined command and control (C2) and combat support capabilities. The integration of Service and Agency-developed data sources and decision support tools is essential to the Combatant Commanders' abilities to "fight joint." These products must support both fixed-base and deployed decision makers on diverse platforms and under communications conditions ranging from robust to austere. DISA's own joint C2 capabilities are focused on enabling the readiness, planning, mobilization support, deployment, execution, and sustainment of deployed forces. In addition, DISA provides the infrastructure that integrates those Service and Agency products, to include common distributed track object services, messaging, applications management, data access and translation, and collaboration services.

Through the Global Command and Control System (GCCS), DISA enables joint operations planning and execution, global access to readiness data, situational awareness via a common operational picture, and collaboration and decision support capabilities for Combatant Commanders as well as many joint force commanders. GCCS components form the critical C2 backbone of joint operations, deployed in over 625 locations worldwide, supporting more than 10,000 joint and coalition workstations. Lighter, configurable deployments of GCCS - such as the Bosnia Operational Picture - support selected Joint Task Forces and coalition operations. C2 systems at all levels gain significant interoperability across components and increased effectiveness by leveraging a common suite of tools and infrastructure components provided by the Common Operating Environment (COE). Today 125 C2 systems either use the COE or plan to deploy on it.

DISA is deeply involved today in Advanced Concept Technology Demonstrations (ACTDs) working with the Combatant Commanders to pilot key capabilities essential to the ongoing transformation. These ACTDs respond to high-priority capability shortfalls involving complex conceptual or technical issues appropriately addressed early in a technology lifecycle. Active ACTDs include: Adaptive Courses of Action, Combatant Commander for the 21st Century, C4I for the Coalition Warrior, Joint Logistics, Joint Theatre Logistics, Automated Intrusion Detection, Homeland Security C2, and Coalition Rear Area Security Operations Command and Control. This last ACTD is already providing shared force protection situation awareness at more than 10 locations worldwide in support of Operation Enduring Freedom.

Contact Info: DISA Public Affairs Office: (703) 607-6900;

Website: http://www.disa.mil

Last Updated: December 2005

Return to Contents

National Security Agency (NSA)

Mission.

The National Security Agency/Central Security Service (NSA/CSS) is a Combat Support Agency of the Department of Defense (DOD). It implements the SecDef's responsibility as executive agent for United States Government signals intelligence and communications security, and it conducts related activities as assigned. The Director of the NSA also serves as the Chief of the Central Security Service (CSS), which provides the Military Services a unified cryptologic organization within the Department of Defense designated to assure proper control of the planning, programming, budgeting, and expenditure of resources for cryptologic activities. NSA is the Nation's key cryptologic organization. It provides and protects vital information from the battlefield to the White House. It assures the security of U.S. signals and information systems and provides intelligence derived from those of the Nation's adversaries. NSA is headquartered at Fort Meade, MD.

The resources of NSA are organized for the accomplishment of two Principal missions:

- The **Information Assurance** mission provides the solutions, products, and services, and conducts defensive information operations, to achieve information assurance for information infrastructures critical to U.S. national security interests.

- The **Foreign Signals Intelligence** or SIGINT mission allows for an effective, unified organization and control of all the foreign signals collection and processing activities of the United States. NSA is authorized to produce SIGINT in accordance with objectives, requirements, and priorities established by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board.

History.

NSA was created in November 1952. Its immediate predecessor, the Armed Forces Security Agency (AFSA), was established under the Joint Chiefs of Staff, in 1949 and was to be responsible for directing the communications and electronic intelligence activities of the military intelligence units - the Army Security Agency, Naval Security Group and the Air Force Security Service. However, the agency had little power and lacked a centralized coordination mechanism. NSA's authority and organizational structure remedied AFSA's deficiencies. NSA coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. NSA is also one of the most important centers of foreign language analysis and research within the government.

Information Assurance Directorate (IAD).

Information Assurance Directorate's mission includes:

- Detecting, reporting, and responding to cyber threats.
- Providing OPSEC assistance and training, both inside and outside DoD through the Interagency OPSEC Support Staff.
- Making encryption codes to securely pass information between systems.
- Embedding IA measures directly into the emerging Global Information Grid.
- Building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions.
- Testing the security of customers' systems.
- Evaluating commercial software and hardware against nationally set standards.

The information assurance component of Information Operations assures DOD's operational readiness by providing for the continuous availability and reliability of information systems and networks. IA protects the Defense Information Infrastructure against exploitation, degradation, and denial of service, while providing the means to efficiently reconstitute and reestablish vital capabilities following an attack.

IAD Interagency OPSEC Support Staff (IOSS)

Operations Security (OPSEC) is an analytic process used to deny an adversary information - generally unclassified - concerning U.S. intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. OPSEC is a systematic and proven process used to deny adversaries information about U.S. capabilities and intentions by protecting unclassified information about sensitive activities.

The IOSS is available to assist organizations and individuals inside DOD, and in government departments and agencies outside, with OPSEC materials, training, operations analysis, and implementing the best OPSEC practices for your activities (See contact information for IOSS at the end of this section, below).

The OPSEC process involves five steps:

- Identification of critical information,
- Analysis of threats,
- Analysis of vulnerabilities,
- Assessment of risks, and
- Application of appropriate countermeasures.

IOSS provides OPSEC training, program development assistance, and awareness materials in support of the National OPSEC Program. The IOSS' mission is to promote OPSEC principles and help members of the national security community develop their own self-sufficient OPSEC programs to better protect U.S. programs and activities.

Return to Contents

INFOSEC Assurance Training and Rating Program (IATRP).

NSA developed the IATRP to meet the needs of all potential customers who need INFOSEC Assurances Services. The IATRP is a partnership between NSA and INFOSEC providers (U.S. Government and private sector). The IATRP sets the standard for INFOSEC Assurance Methodology through NSA-sponsored classes. INFOSEC Assessments. A high-level review of the Information Systems Security (INFOSEC) posture of an organization to identify potential vulnerabilities. NSA has the authority to perform INFOSEC assessments for eligible organizations. Once vulnerabilities are identified, NSA will provide recommendations for their elimination or mitigation.

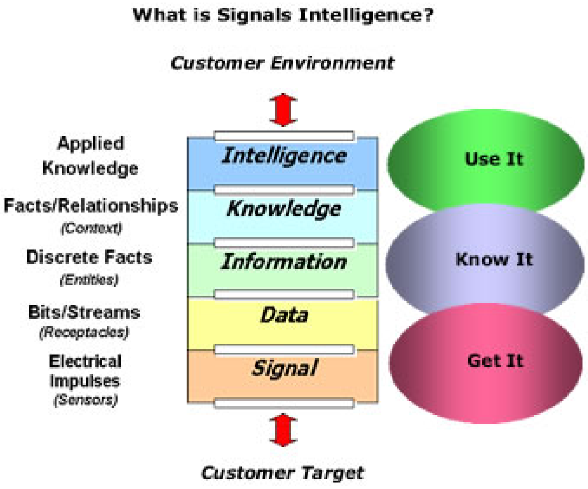
Signals Intelligence (SIGINT).

The National Security Agency collects, processes and disseminates foreign Signals Intelligence (SIGINT). NSA provides information in the form of SIGINT products and services that enable our government to make critical decisions and operate successfully.

SIGINT is derived from the signals environment that is described by the graphic above. Other agencies within the Intelligence Community are responsible for other types of intelligence:

- Human Intelligence (HUMINT) is primarily the responsibility of the Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA),
- Imagery Intelligence (IMINT) belongs to National Geospatial-Intelligence Agency (NGA),
- Military Intelligence and Measurement and Signature Intelligence (MASINT) belongs to DIA.

A unique discipline, SIGINT's modern era dates to World War II, when the U.S. broke the Japanese military code and learned of plans to invade Midway Island, allowing the U.S. to defeat Japan's superior fleet. The use of SIGINT is believed to have directly contributed to shortening the war by at least one year. NSA employs the country's premier cryptologists. It is said to be the largest employer of mathematicians in the United States and perhaps the world. Its mathematicians contribute directly to the two missions of the Agency: designing cipher systems that will protect the integrity of U.S. information systems and searching for weaknesses in adversaries' systems and codes.



The National Cryptologic School provides unique training for the NSA workforce, and serves as a training resource for the entire Department of Defense. NSA sponsors employees for bachelor and graduate studies at the Nation's top universities and colleges, and selected Agency employees attend the various war colleges of the U.S. Armed Forces.

Research And Development (R&D).

NSA conducts one of the U.S. government's leading R&D programs. Some have significantly advanced the state of the art in the scientific and business worlds. NSA's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to the modern computer. NSA pioneered efforts in flexible storage capabilities, which led to the development of the tape cassette.

NSA also made ground-breaking developments in semiconductor technology and remains a world leader in many technological fields.

Most NSA/CSS employees, both civilian and military, are headquartered at Fort Meade, Maryland, centrally located between Baltimore and Washington, DC. Its workforce represents an unusual combination of specialties: analysts, engineers, physicists, mathematicians, linguists, computer scientists, researchers, as well as customer relations specialists, security officers, data flow experts, managers, administrative officers and clerical assistants.

Contact Information:

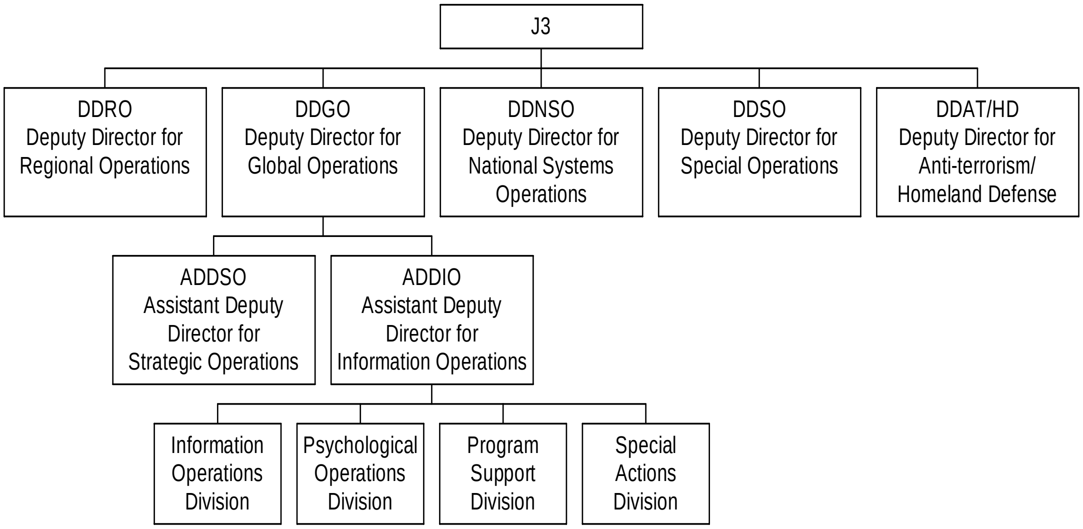
- NSA Information Assurance Service Center (NIASC): (800) 688-6115
- NSA Interagency OPSEC Support Staff: (443) 479-4677
- Infosec Assessment Training And Rating Program (IATRP): 410-854-7821

Website: http://www.nsa.gov/

Updated: December 2005

Return to Contents

Joint Staff, Deputy Director of Global Operations (DDGO)



J3

DDRO Deputy Director for Regional Operations

DDGO Deputy Director for Global Operations

DDNSO Deputy Director for National Systems Operations

DDSO Deputy Director for Special Operations

DDAT/HD Deputy Director for Anti-terrorism/ Homeland Defense

ADDSO Assistant Deputy Director for Strategic Operations

ADDIO Assistant Deputy Director for Information Operations

Information Operations Division

Psychological Operations Division

Program Support Division

Special Actions Division

Staff Mission: The Deputy Director for Global Operations (DDGO) is tasked to provide the Director of Operations and the Chairman of the Joint Chiefs of Staff the expertise and advice in coordinating joint global operations to include information operations. Within the DDGO, the Assistant Deputy Director for Information Operations is responsible for IO activities, developing joint doctrine for IO, and coordinating with the Office of the Secretary of Defense, combatant commands, Services, other staff directorates and across the Intelligence Community and Inter-Agency on IO issues/actions. In addition, the ADDIO is the focal point for all special technical operations.

Organization: The Directorate For Global Operations contains the following four IO divisions:

- Information Operations
- Psychological Operations
- Program Support
- Special Actions.

The Information Operations Division consists of the following branches: Combatant Command Special Technical Operations (STO) Support, Plans Support, Computer Network Computer Network Operations (CNA, CND, CNE, IA and CND-RA) , Electronic Warfare, Intelligence Community Liaisons , and Science and Technology.

The Psychological Operations Division consists of the Programs and Doctrine and the Combatant Command Support branches.

The Program Support Division consists of the following branches: Policy/Doctrine, and Special Technical Operations (STO) Procedures, Automated Information Systems/Budget, and Network Support.

Return to Contents

The Special Actions Division consists of Support Activities Branch, and Tactical Security Branch.

Location: The DDGO is located within the Pentagon.

Website: http://www.dtic.mil/jcs/

Last Updated: December 2005.

Joint Spectrum Center (JSC)

Mission: To enable effective and efficient use of the electromagnetic spectrum and control of electromagnetic effects in support of national security and military objectives.

Major Responsibilities

- Provides operational spectrum management support to the Joint Staff and COCOMs for contingency operations, exercises, and otherwise as requested.
- Conducts research and development (R&D) into spectrum efficient technologies to improve the Department's use of spectrum.
- Facilitates global spectrum information exchange by developing protocols, standards, applications, and information systems.
- Implements the DoD Joint Electromagnetic Environmental Effects (E3) Program.
- Develops, maintains, and distributes spectrum engineering and E3 analysis models, simulations, software, and data.
- Develops, distributes, and conducts E3 and spectrum management training courses for DoD Components.
- Provides technical E3 and spectrum engineering support, on a customer funded basis, to DoD, Federal Government organizations, the private sector when it is in the interest of national defense, and to foreign entities when authorized

The major functional components of JSC include the following:

- **J3 Operations Division**. -- provides Communications-Electronics (C-E)/Electromagnetic Battlespace (EMB) support and Joint Spectrum Interference Resolution (JSIR) support to the Joint Staff, Unified Combatant Commands, and warfighting commanders. This support is available for both contingencies and joint training exercises and can be provided from the JSC or on-site.

- **J5 Electromagnetic Environmental Effects Engineering Division**. -- manages the Joint DoD E3 Program. The primary goal of this program is to ensure that weapon systems and other equipment provided to our Warfighters are electromagnetically compatible with the battlefield electromagnetic EM environment and are supportable in the Electromagnetic Spectrum (EMS). The major divisions of the E3 program are: Milestone Decision Authority (MDA) Acquisition Support, EMCS Lead Standardization activity, E3 Awareness and Training, Joint Service Ordnance E3 program, and DOT&E Program Support.

- **J6 Spectrum Management Information Technology Division**. -- supports the warfighter by providing and maintaining Spectrum Planning Services, E3 Models and Simulations, and Information Systems.

- **J7 Plans and Resources**. -- Promote warfighter access to the electromagnetic spectrum in support of national security and military objectives by providing spectrum strategic policy and regulatory advice, engineering technical and analytical assistance to the Department of Defense, and supporting the personnel, financial, and security requirements of the Joint Spectrum Center.

JSC Tasks and Products: -- these include the following,

<u>JSC Liaison and Coordination Support to Information Operations and Electronic Warfare</u> -- provides direct support to Unified Combatant Commands, Joint Task Forces, and Joint Staff Information Operations/Electronic Warfare (IO/EW) cells, and indirect support for operational military IO/EW planning provided through the Joint Information Operations Center (JIOC), Service IO activities, and IO/EW elements of the Intelligence Community. This effort is conducted under the mission area of "supporting electronic protect missions of information warfare as they relate to spectrum supremacy". The support provided ranges from EW de-confliction analyses to supporting IO red team efforts as they relate to spectrum dependent matters.

<u>Support to the Warfighting Unified Combatant Commands and JTF Commanders</u> -- includes:

- Support to the Electronic Warfare officer and the information operations (IO) cell
- JSC liaison and coordination support to IO cell, Joint Information Operations Center (JIOC), and Intelligence organizations as required
- Automated frequency management support and training, electromagnetic environmental database support, electromagnetic compatibility (EMC) analysis support
- Generation of the Joint Communications Electronics Operation Instruction (JCEOI)
- Development of the Joint Restricted Frequency List (JRFL)
- Joint Spectrum Interference Resolution (JSIR) support through analysis and deployment teams as necessary
- Area Studies in support of Unified Combatant Command requirements (see below)
- Review of operations plans (OPLANS) for spectrum supportability, upon request.

<u>Area Studies in Support of Unified Combatant Command Requirements</u>. Each year, the Joint Spectrum Center (JSC) produces area studies for various countries, on CD-ROM, that provide information on the physical and

cultural characteristics and the civil telecommunications sector. Specific items addressed include: frequency management; broadcasting; telephone, telegraph, and telex; data communications; aeronautical communications; maritime communications; and transmission systems. Frequency allocations, assignments, histograms, and site location maps are also included. Frequency assignment data is also provided on the CD-ROM in a spreadsheet.

Electromagnetic Battlespace and Communications-Electronics Planning Support: supports achieving information superiority and full spectrum dominance by providing services and products to Assistant Secretary of Defense for Networks and Information Integration (NII), Joint Staff, Unified Commands, Joint Task Forces, Military departments, and Defense Agencies to enable the DoD's effective use of the electromagnetic spectrum. Providing electronic battlespace and C-E planning support directly to the warfighter, the JSC Operations Division offers these typical services:

- SPECTRUM XXI Frequency Nomination/Assignment/Allotment
- Electronic Warfare De-confliction
- Joint Restricted Frequency List (JRFL) Assistance/Preparation
- Interference Analysis
- Propagation Predictions (MF-EHF)
- C-E System Performance Prediction
- Radar Target Acquisition Coverage Prediction
- EMC Analyses in Support of Frequency Planning
- Topographical Analyses
- JCEOI Planning/Preparation
- Electromagnetic Environment (EME) Definition
- Geophysical Environment Definition.

Joint Spectrum Interference Resolution (JSIR): Established by DoD in October 1992 as a replacement for the electromagnetic interference portion of the former DoD Meaconing*, Intrusion, Jamming, and Interference (MIJI) program. MIJI’s focus was on the reporting of potentially hostile electronic warfare attacks against U.S. military systems. The JSIR program is structured to have interference incidents resolved at the lowest possible level of the component chain of command, using component organic resources to resolve interference incidents where possible. Those incidents that cannot be resolved locally are referred up the chain of command, with resolution attempted at each level. If the interference incident cannot be resolved by the affected DoD Component or the service engineering agency responsible for spectrum interference resolution, then it is referred to the JSC JSIR office for resolution.

* [NOTE: Meaconing is defined (per FM 24-33, “Communications Techniques: Electronic Counter-Countermeasures”, July 1990) as the transmission or retransmission of actual or simulated navigation signals to confuse navigation. Meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations].

C2-Protect Support: The JSC Operations Division supports C2-Protect operations through each of the following activities:

- Provision of databases on friendly force C2 system location and technical characteristics data for use in planning C2-protect. The databases cover DoD, US government, and civilian communications, as well as radar NAVAIDS, broadcast, identifications, and electronic warfare (EW) systems. The databases are available on a quick reaction basis in a variety of formats and media to meet the needs of IO planners and spectrum managers.

- Assistance to the EW officer or IO cell in the development of the JRFL. The JSC provides an automated tool, SPECTRUM XXI, to assist in the development and management of the JRFL. The JSC has Unified Combatant Command support teams that deploy to the combatant command or JTF. The teams are available to prepare the JRFL or provide training and assistance in JRFL preparation. These teams are also available to provide assistance in spectrum management matters.

- Assistance in the resolution of operational interference and jamming incidents through the auspices of the JSIR Program

- Provision of databases on foreign C3 frequency and location data. This data is developed primarily from open sources

- Provision of unclassified C3 area studies. The studies are unclassified, developed entirely from open source material, and address the C3 infrastructure of over 100 countries. The studies provide information on the physical and cultural characteristics (geography, climate, and population), overview of telecommunications systems, and the frequencies used by each country. Data is provided on civilian, military, radio/TV broadcast and navigational systems. The frequency data is provided in automated form and can be used directly by spectrum management tools such as the widely used SPECTRUM XXI.

Spectrum Regulatory Support. The growth of commercial wireless services, such as Personal Communications Services, has greatly increased the demand for spectrum, and increased pressure for the government to relinquish portions of the spectrum to commercial interests. Continuing pressure to reallocate portions of the spectrum requires that the DoD have the ability to quickly assess the operational and economic impact of proposed reallocation legislation in order to defend critical DoD spectrum. J7 draws upon a collection of databases and experience with spectrum management to respond to ad hoc inquiries. In addition, the J7 is positioned to develop in-depth assessments of various reallocation proposals that will provide all levels of government with the information needed to make responsible reallocation decisions.

Leadership: The command billet of the center rotates between the Army, Air Force and Navy O-6. The Commander, JSC reports to the Principal Director for Operations at DISA.

Location: David Taylor Research Center, 2004 Turbot Landing, Annapolis, Maryland.

Phone: (410) 293-2457, DSN 281-2457

Website: http://www.jsc.mil/

Last updated: October 2005

Return to Contents

Joint Warfare Analysis Center (JWAC)

Mission: provides combatant commands, Joint Staff, and other customers with precise technical solutions in order to carry out the national security and military strategies of the United States. JWAC maintains and enhances its ability to conduct comprehensive technical analysis. Over the subsequent quarter of a century, JWAC has evolved from a small program office into a joint command of more than 600 personnel. As it grew, it became part of the Joint Chiefs of Staff in 1994 and then was spun-off as an independent joint command subordinate to Joint Forces Command (formerly Atlantic Command) in 1998.

Tasks:

- Provides Combatant Commander planners with full-spectrum analytical products in support of their objectives and guidance.

- Interfaces with the Joint Staff, national intelligence agencies, military commands, and governmental agencies to acquire necessary intelligence.

- Develops and adapts modeling and simulation technologies for analysis, computation, and the presentation of options to combatant commands, the Joint Staff, and other customers through partnership with DoD and Industry technology centers of excellence.

- Assesses strategic and operational planning processes including non-traditional methods for achieving national security objectives.

- Conducts combat assessment through the National Military Joint Intelligence Center Federated BDA Architecture.

Capabilities:

- Maintains direct liaison staffs with Combatant Commanders, Joint Staff, DoD and non-DoD agencies. Liaison deploys in theater during crises and exercises.

- Develops mathematical models, system simulation studies, and data-gathering methods and techniques to support analysis of system and component (subsystem) performance characteristics and interdependencies among different system types.

- Researches political and socioeconomic conditions in countries of interest.

- Develops data-gathering and analysis methods and techniques to assess military, political, and socioeconomic impacts of U.S. military action and mathematical model and system simulation to support this analysis.

- Participates in development of new methodologies and technologies in support of joint experimentation, wargaming, and precision engagement.

Subordination: JWAC reports to the U.S. Joint Forces Command, Norfolk VA.

Leadership: Command of JWAC rotates between a Navy and Air Force O-6.

Personnel: The JWAC workforce is comprised of over 600 employees; approximately 500 are civilian and contractor positions, including multidisciplinary scientists, engineers, and analysts and the Command is authorized 62 military billets.

Location: JWAC is located at the Naval Support Facility, Dahlgren VA.

Note: The unclassified information above was obtained and approved by the JWAC for inclusion in this publication. Additional information may be obtained at:

Website: http://www.jwac.mil/

Last Updated: January 2005.

Information Assurance Technology Analysis Center (IATAC)

IATAC

The Information Assurance Technology Analysis Center (IATAC) is a U.S. Department of Defense Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC), which is a DoD Field Activity under the Under Secretary of Defense for Acquisition, Technology and Logistics, reporting to the Director, Defense Research & Engineering (DDR&E).

Mission :

Provide the DoD a central point of access for information on Information Assurance (IA) emerging technologies in system vulnerabilities, research and development, models, and analysis to support the development and implementation of effective defense against Information Warfare attacks.

Management and Direction of IATAC Operations:

IATAC operates under the direction of our Government Steering Committee. The committee is made up of individuals from various government organizations, the Department of Defense, and the research and development (R&D) and science and technology (S&T) , operational, and governance communities; this includes representation from the Defense-Wide Information Assurance Program (DIAP), Joint Task Force for Global Network Operations (JTF-GNO), National Security Agency (NSA), Naval Postgraduate School (NPS), Office of the Secretary of Defense (OSD), and the Naval Information Warfare Center – Norfolk (NIOC-Norfolk). The steering committee meets at least once a year and provides input and feedback on IATAC’s operations, particularly our information collection and information dissemination efforts. Additionally, the committee reviews topics for proposed technical reports.

History:

The United States is vulnerable to Information Warfare attacks because our economic, social, military, and commercial infrastructures demand timely and accurate as well as reliable information services. This vulnerability is complicated by the dependence of our DoD information systems on commercial or proprietary networks which are readily accessed by both users and adversaries. The identification of the critical paths and key vulnerabilities within the information infrastructure is an enormous task. Recent advances in information technology have made information systems easier to use, less expensive, and more available to a wide spectrum of potential adversaries.

Our nation’s information infrastructure depends on the survivability, authenticity, and continuity of DoD information systems. These systems are vulnerable to external attacks, due in part to the necessary dependence on commercial systems and the increased use of the Internet. The survivability, authenticity, and continuity of DoD information systems is of supreme importance to the Warfighter. With the increasing amount of concern and Information Warfare activities requiring rapid responses, it is difficult to ensure that all appropriate agencies and organizations are given the knowledge and tools to protect from, react to, and defend against Information Warfare attacks. IATAC was established under the direction of DTIC and the integrated sponsorship of the Defense Information Systems Agency (DISA); the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII)); the Joint Staff (J6); and DDR&E, whose missions direct the DoD's responses, developments, and operations regarding IA.

Return to Contents

IATAC provides a central authoritative source for IA vulnerability data, information, methodologies, models, and analyses of emerging technologies relating to the survivability, authenticity, and continuity of operation of information systems critical to the nation's defense in support of the Warfighter's front line missions. IATAC's support extends across the spectrum from policy, doctrine, and strategy development, to R&D, S&T, engineering, and architecture, to operations and training. This spectrum of activities ensures the collection, analysis, and dissemination of a broad and growing library of scientific technical information (STI) related to IA. IATAC serves to help synchronize DoD's IA efforts across that entire spectrum of activities as well as into the civil/federal government.

IATAC operates as a specialized subject focal point, supplementing DTIC services within DoD Directive 3200.12, DoD Scientific and Technical Information Program (STIP), dated 15 February 1983.

Location and Contact Information:
IATAC
3190 Fairview Park Drive, 9th Floor,
Falls Church, VA 22042
Phone: (703) 289–5454
Fax: (703) 289–5467
E-mail: iatac@dtic.mil

Website: iac.dtic.mil/iatac/

Last Updated: December 2005

U.S. Strategic Command (USSTRATCOM)

One of nine U.S. unified commands under DoD; the USSTRATCOM commander leads the nation's strategic capabilities.

Mission: Provide the nation with global deterrence capabilities and synchronized DoD effects to combat adversary weapons of mass destruction worldwide. Enable decisive global kinetic and non-kinetic combat effects through the application and advocacy of integrated intelligence, surveillance and reconnaissance (ISR); space and global strike operations; information operations; integrated missile defense and robust command and control. USSTRATCOM combines the synergy of the U.S. legacy nuclear command and control mission with responsibility for space operations; global strike; Defense Department information operations; global missile defense; and global command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR). This provides a unified resource for greater understanding of specific threats around the world and the means to respond to those threats rapidly.

History: The current USSTRATCOM resulted from the Oct. 1, 2002 integration of two previous unified commands: U.S. Space Command, which oversaw DoD space and information operations; and the former USSTRATCOM, responsible for the command and control of U.S. strategic forces. USSTRATCOM was as the lead Combatant Command for integration and synchronization of DoD-wide efforts in combating weapons of mass destruction in January 2005.

Location: Headquartered at Offutt Air Force Base, NE, with units at Cheyenne Mountain Air Force Station, CO. (Cheyenne Mountain Operations Center); Lackland AFB, TX (Joint Information Operations Center); and Arlington, VA. (Joint Task Force -- Global Network Operations).

Headquarters Organizational Structure:

The command headquarters comprises more than 2,500 people, representing all four services, plus DoD civilians and contractors. The command is organized under a modified J-code structure as follows:

- **J0 (Office of the Commander, and the staff support agencies)** - responsible for establishing the goals, mission, vision and leadership of the command. To help the commander, the immediate staff also includes the deputy commander in chief and a group of special advisors.

- **J1 (Manpower and Personnel)** - develops and administers USSTRATCOM command manpower and personnel policies, human resources, and personnel assignment programs.

- **J3 (Global Operations)** - coordinates the planning, employment and operation of DoD strategic assets and combines all current operations, global command and control and intelligence operations.

    - **J2 (Intelligence)** - apprises the commander of foreign situations and intelligence issues relevant to current operational interests and potential national security policies, objectives and strategy. This includes providing indications, warning and crisis intelligence support, supporting unified command intelligence requirements, developing doctrine, joint architecture, coordinating support requirements and providing targeting support.

  - **J3B (Current Operations)** - operates the Global Operations Center to provide the commander and the J3 with situational awareness, command and control, and integration across all mission areas. Conducts mission analysis, leads course of action development, and performs contingency and crisis action planning. Executes missions as directed by the Secretary of Defense and the President.

  - **J4 (Logistics)** - Plans, coordinates and executes logistics functions for mobility, maintenance, engineering, readiness and sustainment and munitions management.

  - **J6 (C4 Systems)** - coordinates, facilitates, monitors and assesses systems, networks and communications requirements.

- **J5 (Plans and Policy)** – coordinates development and implementation of national security policy as it applies to USSTRATCOM mission. Develops future concepts for military space operations; global strike; information operations; global missile defense; and command and control, communications, computers, intelligence, surveillance and reconnaissance as outlined in the Unified Command Plan. Integrates and synchronizes deliberate planning efforts. Prepares and maintains national strategic nuclear war plan, and provides integrated global strike planning to deliver rapid, extended range, precision kinetic (nuclear and conventional) and non-kinetic (elements of space and information operations) effects in support of theater and national objectives. Performs day-to-day activities required for crisis-action and deliberate planning and execution, with updates to plans as necessary.

- **J8 (Capability and Resource Integration)** - conducts force management and analysis to include integrating, coordinating, prioritizing, and advocating command future concepts, mission capability needs, weapons system development, support for emerging technologies, and command and control architecture across the mission areas. Responsible for articulation and development of all command requirement processes, and ensures appropriate decision support tools and assessment processes are in place to enhance operational capabilities; includes comptroller support, concepts and experimentation, and force assessments.

As DoD's key advocate for global capabilities, the command has extensive ties with defense agencies, the Department of Energy's national laboratories, and other sources of support. Through its many contacts and interagency relationships, the command facilitates planning, enhances information sharing between the military and other government agencies and streamlines decision making.

USSTRATCOM Functional Components, Service Components and Task Forces:

USSTRATCOM exercises command authority over four joint functional component commands (JFCCs) responsible for day-to-day planning and execution of primary mission areas: space and global strike; intelligence, surveillance and reconnaissance; network warfare; integrated missile defense; and combating weapons of mass destruction.

- **JFCC - Integrated Missile Defense (JFCC-IMD)** Commander, U.S. Army Space and Missile Defense Command/Army Forces Strategic Command, also serves as the commander for the JFCC-IMD; is responsible for meeting USSTRATCOM's Unified Command Plan responsibilities for planning, integrating, and coordinating global missile defense operations and support. It conducts the day-to-day operations of assigned forces and coordinates activities with associated combatant commands, other STRATCOM JFCCs and the efforts of the Missile Defense Agency.

- **JFCC - Intelligence, Surveillance and Reconnaissance (JFCC-ISR) --** Commander, JFCC-ISR, also serves as the *Director, Defense Intelligence Agency*. This component is responsible for coordinating global intelligence collection to address DoD worldwide operations and national intelligence requirements. It will serve as the epicenter for planning, execution and assessment of the military's global Intelligence, Surveillance, and Reconnaissance operations; a key enabler to achieving global situational awareness.

- **JFCC - Network Warfare (JFCC-NW)** -- Commander, JFCC-NW also serves as *Director, National Security Agency*. This component facilitates cooperative engagement with other national entities in computer network defense and offensive information warfare as part of the global information operations mission. This coordinated approach to information operations involves two other important supporting commands. The *Director, Defense Information Systems Agency also heads the Joint Task Force for Global Network Operations(JTF-GNO)*, which is responsible for operating and defending U.S. worldwide information networks, a function closely aligned with the efforts of the Joint Functional Component Command for Network Warfare.

- **JFCC - Space & Global Strike (JFCC-SGS)** -- Commander 8th Air Force serves as JFCC-SGS, headquartered at Offutt Air Force Base, NB; integrates all elements of military power to conduct global strike effects and also direct the deliberate planning and execution of assigned space operation missions. For plans not aligned with a specific mission set, the JFCC-SGS will work in close coordination with USSTRATCOM headquarters as lead responsible for the integration and coordination of capabilities provided by all other Joint Functional Component Commands.

- **Joint Information Operations Center** -- integrates Information Operations (IO) into military plans and operations across the spectrum of conflict. Located at Lackland AFB, TX, JIOC deploys IO planning teams worldwide to support combatant commanders and joint task forces.

- **Combating Weapons of Mass Destruction** -- As this initiative is in its very formative stages, USSTRATCOM has yet to formalize any specific componency structure. There are detailed issues to work through, including the proper distribution of subject matter expertise and an assessment of expanding relationships with other U.S. government departments and foreign nations.

- **Joint Task Force-Global Network Operations (JTF-GNO)** -- Located in Arlington, VA is USSTRATCOM's operational component supporting defense of DoD's information infrastructure. This is done by integrating GNO capabilities into the operations of all DoD computers, networks, and systems.

- **Air Force Space Command (AFSPC)** -- provides space forces and trained ICBM forces; has two numbered air forces: 14th Air Force (Vandenberg AFB, CA) that provides space warfighting forces, and 20th Air Force (Warren AFB, WY) that operates assigned ICBM weapon systems. AFSPC provides ballistic missile warning information, operates the Space Warfare Center, and is responsible for DoD's ICBM follow-on operational test and evaluation program; also operates the Global Positioning System, Defense Satellite Communications Systems Phase II and III, Defense Meteorological Support Program, Defense Support Program, NATO III and IV communications and Fleet Satellite Communications System UHF follow-on and MILSTAR satellites. AFSPC also provides continuous, real-time solar flare warnings, and operates the worldwide Air Force Satellite Control Network of satellite tracking and communications link stations to satellites. .

- **U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (SMDC/ARSTRAT)** --, headquartered in Arlington, VA; is the Army service component to USSTRATCOM, conducts space operations and provides planning, integration, control, and coordination of Army forces and capabilities in support of USSTRATCOM; serves as proponent for space and ground-based midcourse defense and as Army operational integrator for global missile defense; conducts mission related research, development, and acquisition in support of Army Title 10 responsibilities and serves as the focal point for desired characteristics and capabilities in support of USSTRATCOM missions.

- **Marine Corps Forces U.S. Strategic Command (MARFORSTRAT)** -- serves as the U. S. Marine Corps service component to the Commander, USSTRATCOM. Particular focus is advising USSTRATCOM, subordinate Joint Force Commanders, functional component and service component commanders on the proper employment of U.S. Marine Corps forces and capabilities.

- **Fleet Forces Command** -- headquartered in Norfolk, Va., is the U.S. Navy component of U.S. Strategic Command. Fleet Forces Command is responsible for the Atlantic Ocean, the Caribbean Sea and the waters around Central and South America extending in the Pacific to the Galapagos Islands; provides forces to support U.S. and NATO commanders. Additionally, Fleet Forces Command provides readiness training, and logistical/administrative support for its ships and aviation squadrons.

- **Aerial Refueling/Tankers** – enhance USSTRATCOM’s worldwide reach; assigned to 18th Air Force, Scott AFB, Ill., with headquarters at Air Mobility Command, Scott AFB, IL.

- **Airborne Communications** -- Navy E-6B aircraft, assigned to Strategic Communications Wing One, Tinker AFB, Okla., provide survivable communications link between national decision-makers and the nation's strategic forces. An airborne command post, the E-6B enables the President and the Secretary of Defense to directly contact crews on the nation's ballistic missile submarines, land-based intercontinental ballistic missiles and long-range bombers.

- **Ballistic Missile Submarines** -- Navy ballistic missile submarines, (SSBNs), provide launch capability from around the globe using the Trident missiles. Atlantic SSBNs are based at Kings Bay, Ga., (headquarters at Norfolk, VA); Pacific SSBNs are based at Bangor, Wash., (headquarters at Pearl Harbor, HI).

- **Strategic Bomber and Reconnaissance Aircraft** -- 8th Air Force, (Barksdale AFB, LA), can deploy to any area of the world. B-52 bombers are based at Barksdale AFB, LA, and Minot AFB, ND. B-2 stealth bombers are stationed at Whiteman AFB, Mo. Worldwide reconnaissance aircraft assigned to 8th AF that support the USSTRATCOM mission include the RC-135 Rivet Joint (Offutt AFB, Neb.), and the U-2S (Beale AFB, CA).

- **Land-based Intercontinental Ballistic Missiles** -- Air Force ICBMs, dispersed in hardened silos across the U.S. central tier, provide a quick-reacting, highly reliable component to the nation's strategic forces. Minuteman III missile launch control centers are based from Warren AFB, WY; Malmstrom AFB, MT; and Minot AFB, ND. ICBM crews report to 20th Air Force, at Warren AFB.

Website: www.stratcom.mil

Last Updated: November 2005

U.S. Special Operations Command (USSOCOM)

USSOCOM is one of the nine U.S. unified commands under DOD. It organizes, trains, and equips special operations forces provided to Geographic Combatant Commanders, American Ambassadors and their country teams. USSOCOM manages and oversees all CONUS-based SOF: the Air Force Special Operations Command, the Naval Special Warfare Command, the US Army Special Operations Command, and the Joint Special Operations Command. USSOCOM also develops SOF-specific tactics, techniques, procedures, and doctrine, and conducts research, development, and acquisition of SOF-peculiar equipment. USSOCOM ensures its forces are trained and "joint-ready" to respond to the call from the President, Secretary of Defense and the other eight combatant commanders as necessary.

Mission. USSOCOM leads, plans, synchronizes, and as directed, executes global operations against terrorist networks. USSOCOM trains, organizes, equips and deploys combat ready special operations forces to combatant commands.(delete: directs, and executes special operations in the conduct of the War on Terrorism in order to disrupt, defeat, and destroy terrorist networks that threaten the United States, its citizens and interests worldwide).

Special operations are operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement. These operations often require covert, clandestine, or discreet capabilities. Special operations are applicable across the range of military operations. They can be conducted independently or in conjunction with operations of conventional forces or other government agencies and may include operations by, with, or through indigenous or surrogate forces. Special operations differ from conventional military actions in the following ways:

- Greater degree of physical and political risk
- Unique operational techniques, mode of employment, and independence from friendly support
- Detailed operational intelligence and indigenous assets

Special Operations Forces Core Tasks
- (Counterterrorism (CT)) Counter Proliferation of WMD
- (Counter Proliferation (CP)) Counterterrorism (CT)
- Special Reconnaissance (SR)
- Direct Action (DA)
- Unconventional Warfare (UW)
- Foreign Internal Defense (FID) (Information Operations (IO))
- Civil Affairs Operations (CAO) (Psychological Operations (PSYOP))
- Information and Psychological Operations (Foreign Internal Defense (FID))
- Synchronize DOD efforts in the GWOT (Civil Affairs Operations (CAO))

USSOCOM responsibilities (per Title 10, U.S. Code) include the following:
- Develop Strategy, Doctrine & Tactics

- Train assigned forces
- Conduct specialized courses of instruction for commissioned and noncommissioned officers
- Validate and establish priorities for requirements
- Ensure the interoperability of equipment and forces
- Ensure combat readiness of forces assigned to USSOCOM
- Monitor the preparedness of special operations to carry out assigned missions of SOF assigned to unified combatant commands other than USSOCOM

History. USSOCOM was established as a unified combatant command at MacDillAFB, FL, in April 1987. Concerns about interoperability problems both between the services and in the integration of SOF into joint operations led to passage of the 1986 Goldwater-Nichols Defense Reorganization Act. The Cohen- Nunn Amendment to the DoD Authorization Act of 1987, established USSOCOM and the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (SO/LIC).

Components. USSOCOM has (three) four component commands and one sub-unified command:

1. U.S. Army Special Operations Command (USASOC). Located at Ft. Bragg, North Carolina. USASOC's mission is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned active duty and Reserve Components of the Army Special Operations Force. Their mission is to accomplish special operations, psychological operations, and civil affairs operations as assigned by the Commander, USSOCOM and/or Geographic Combatant Commanders employing SOF. Their forces include:

- U.S. Army Civil Affairs and Psychological Operations Command (Airborne).
  - 4th PSYOP Group (4th POG)
  - 2nd POG and 7th POG (U.S. Army Reserve)
  - 96th Civil Affairs Battalion
  - 350th, 351st, 352, and 353 Civil Affairs Commands (U.S. Army Reserve)

- United States Special Forces Command (Airborne).
  - 1st, 3rd, 5th , 7th, and 10th Special Forces Groups
  - 19th and 20th Special Forces Groups (Army National Guard)

- John F. Kennedy Special Warfare Center and School.

- 75th Ranger Regiment, Fort Benning, Georgia.
  - 1st, 2nd, and 3d Ranger battalions

- 160th Special Operations Aviation Regiment located at Fort Campbell, Kentucky.
  - 1st, 2nd, and 3d Squadrons

- Special Operations Support Command located at Fort Bragg, North Carolina.
  - 528th Support Battalion
  - 112th Signal Battalion

2. Naval Special Warfare Command (NAVSPECWARCOM) Located at Naval Amphibious Base, Coronado, CA. The mission of NAVSPECWARCOM is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned forces in support of joint and fleet operations worldwide. SEAL Teams are maritime, multipurpose combat forces organized, trained and equipped to conduct a variety of special missions in all operational environments and threat conditions. They infiltrate their objective areas by fixed and rotary-winged aircraft, Navy surface ships, combatant craft and submarines. SEAL special mission areas include unconventional warfare, direct action, counter-terrorism, special reconnaissance, foreign internal defense, information warfare, security assistance, counter-drug operations, personnel recovery, and hydrographic reconnaissance.

SEAL Delivery Vehicle (SDV) Teams. Specially trained SEALs and support personnel who operate and maintain SDVs, Dry Deck Shelters (DDS), and the Advanced SEAL Delivery System (ASDS). The ASDS is a dry-submersible vessel that can be launched from a Navy submarine. SDVs are wet submersibles which, along with the ASDS, provide clandestine reconnaissance, direct actions and passenger delivery capability in maritime environments. DDS deliver SDVs and specially trained forces from modified submarines. When teamed with their host submarines, the ASDS, SDV and DDS platforms provide the most clandestine maritime delivery capability in the world.

Special Boat Teams**.** Special Warfare Combatant-craft Crewmen (SWCC) operate and maintain these state-of-the-art, high performance boats used to conduct coastal patrol and interdiction and support special operations missions. Platforms include the Rigid Inflatable Boats, MK-V Special Operations Craft and riverine craft. Focusing on infiltration and exfiltration of SEALs and other SOF, SWCC provide dedicated rapid mobility in shallow water areas where larger ships cannot operate.

Naval Special Warfare (NSW) forces include:

- Naval Special Warfare Group ONE, Coronado, California
- Naval Special Warfare Group TWO, Little Creek, Virginia
- Naval Special Warfare Group THREE, Coronado, California
- Naval Special Warfare Group FOUR, Little Creek, Virginia

3. Air Force Special Operations Command (AFSOC). Located at Hurlburt Field, Florida. It provides Air Force Special Operations Forces for worldwide deployed and assigned to geographic unified commands, conducting the full spectrum of special operations core tasks. The command has the following active duty, Air National Guard, and Air Force Reserve units assigned

- One active duty special operations wing with eight special operations squadrons, including five fixed-wing, one rotary-wing, a combat aviation advisory unit, and a fixed-wing training squadron.
- Two active duty overseas-based special operations groups; Pacific Theater Group is compromised of fixed-wing special operations squadrons and a special tactics squadron and the European Theater Group is compromised of fixed-wing and one rotary-wing special operations squadrons and a special tactics squadron.
- One Air Force Reserve Special Operations Wing with two fixed-wing squadrons.
- One Air National Guard Special Operations Wing with one fixed-wing squadron.
- One active duty special tactics group with four active special tactics squadrons, one Air National Guard special tactics squadron, and an active combat weather squadron.
- One active duty flight test squadron.
- The Air Force Special Operations School.

USAF Special Operations School (USAFSOS)**.** An element of the Joint Special Operations University, the USAF Special Operations School, its mission is to educate U.S. military and other government personnel in the art and science of special operations. It has four academic departments (Asymmetric Warfare, Regional Studies, Joint Special Operations, and Professional Studies), that focus on their respective aspect of special operations. Courses range from three days to two weeks in length and vary in style from large orientation courses to small interactive seminars. USAFSOS faculty also accomplishes advanced academic research in support of the SOF community.

4. Marine Special Operations Command (MARSOC). Located at Camp Lejuene, NC. Stands up 24 February 2006 with a projected strength of 2,600 marines, it's primary mission is to organize, man, train and equip Marine Special Operations Forces. The MARSOC subordinate elements will provide training

to foreign militaries, conduct specified special operations missions like special reconnaissance, engage in direct action, provide intelligence support, coordinate supporting fires and provide logistical support to special operations task forces.

MARSOC will have a headquarters and three subordinate elements:

- The Marine Special Operations Regiment (MSOR) of two battalions.
- The Foreign Military Training Unit (FMTU).
- The Marine Special Operations Support Group (MSOSG).

5. Joint Special Operations Command (JSOC). A sub-unified command of USSOCOM. JSOC provides a joint headquarters to study special operations requirements, ensures interoperability and equipment standardization, develops joint special operations plans and tactics, and conducts joint special operations exercises and training.

IO Core and Related Capabilities within USSOCOM Purview:

Psychological Operations (PSYOP)**.** A vital part of the broad range of U.S. political, military, economic, and ideological activities used by the U.S. government to secure national objectives, PSYOP disseminate truthful information to foreign audiences in support of U.S. policy and national objectives. Used during peacetime, contingency operations, and declared war, these activities are not a form of force, but are force multipliers that use nonviolent means in often violent environments. Persuading rather than compelling physically, they rely on logic, fear, desire or other mental factors to promote specific emotions, attitudes or behaviors. The ultimate objective of U.S. military psychological operations is to convince target audiences to take action favorable to the United States and its allies. The importance and effectiveness of psychological operations has been underscored during OPERATIONS ENDURING FREEDOM and IRAQI FREEDOM.

Civil Affairs (CA). CA units support military commanders by working to minimize the effect of civilians in the battle space and by coordinating with civil authorities and civilian populations in the commander's area of operations to lessen the impact of military operations on them during peace, contingency operations, and declared war. Civil Affairs forces support activities of both conventional and SOF, and are capable of assisting and supporting the civil administration in their area of operations. Long after the guns have fallen silent, the men and women of Civil Affairs continue to provide assistance to foreign governments, and to stabilize regions in turmoil.

Location Address and Contact Information: Headquarters, United States Special Operations Command (HQ, USSOCOM)

- Headquarters, USSOCOM, 7701 Tampa Point Boulevard, MacDill Air Force Base, Florida 33621
- Public Affairs Office: (813) 828-4600

Website: http://www.socom.mil/

Last Updated: December 2005

Joint Task Force – Global Network Operations (JTF - GNO)

MISSION: A component of U.S. Strategic Command (USSTRATCOM), the Joint Task Force - Global Network Operations (JTF-GNO), located in Arlington, VA., is USSTRATCOM's operational component with the mission of directing the operation and defense of the DoD's Global Information Grid (GIG) to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

HISTORY: The JTF-GNO was originally created as the Joint Task Force - Computer Network Defense in December 1998 and was assigned to the United States Space Command (USSPACECOM) in 1999. In 2000, it was redesignated as the Joint Task Force - Computer Network Operations and in October 2002, with the merger of USSTRATCOM and USSPACECOM, JTF-CNO became a component of USSTRATCOM. In June 2004, the Secretary of Defense (SECDEF) ***appointed the Director, Defense Information Systems Agency (DISA) as Commander, JTF-GNO***.

In July 2004, the JTF-GNO formed the Global NetOps Center (GNC) through the functional merger of elements from the JTF-CNO's Operations Directorate, DISA's Global Network Operations and Security Center (GNOSC), the DoD Computer Emergency Response Team (DOD-CERT), and the Global SATCOM Support Center. As such, the GNC is responsible for guiding, directing, and overseeing daily compliance with NetOps policy, providing common defense of the GIG, and ensuring strategic priorities for information are satisfied.

JTF-GNO leads and directs continuous GIG Enterprise Management (GEM), GIG Network Defense (GND), and Information Dissemination Management/Content Staging (IDM/CS). JTF-GNO provides Situational Awareness (SA) of the GIG through the Network Common Operational Picture (NETCOP) and provides customer support to the Chairman, Joint Chiefs of Staff; the National Military Command Center; CDRUSSTRATCOM; and other Combatant Commanders (CCs). The JTF-GNO provides command and control of the GIG under the authority of CDRUSSTRATCOM, through a tiered hierarchy of NetOps Centers working together towards a common goal of assuring Global Decision Superiority by maintaining near real-time SA, end-to-end management, and dynamic DoD network defense.

CURRENT OPERATIONS: The JTF-GNO functions in accordance with Unified Command Plan 2004 and the Joint Concept of Operations for GIG NetOps, assuring Global Information Superiority by achieving the three assurances outlined in the Joint Concept of Operations for GIG NetOps: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery.

Within each theater of operation, the JTF-GNO operates through Theater NetOps Centers (TNCs), established through the functional merger of DISA's Regional Network Operations and Security Centers (RNOSCs), Regional Computer Emergency Response Teams (RCERTs), and Regional SATCOM Support Centers (RSSC). The TNCs establish, maintain, and provide theater-level GIG SA. Also established from this merger is the Global NetOps Support Center (GNSC). The GNSC establish, monitor, and maintain GIG SA view for the global backbone. The GIG Infrastructure Services Management Center (GISMC) was established to facilitate the net-centric transformation of DoD-level enterprise services by optimizing the consolidation and integration of NetOps into existing and emerging applications networks and services. The GISMC develop, monitor, and maintain a GIG SA view of the global infrastructure services to ensure timely and efficient delivery of global information across the GIG.

The GNC is responsible for directing the response to Global NetOps issues and overseeing compliance in accordance with GIG operational policies. The GNC exercises Operational Control (OPCON) of the Theater NetOps Centers (TNC) for Global NetOps issues. The TNCs provide technical support and execution and are Tactical Control (TACON) for Theater NetOps issues to CCs for those parts of the GIG under their control. The TNCs act as the theater focal point to maintain NetOps SA, support the CCs in executing their GIG responsibilities, and serve as liaison between a Theater C4 Control Center (TCCC) or Global C4 Control Center (GCCC) and the JTF-GNO. For Theater NetOps issues, the GNC supports the CCs by ensuring availability of the GIG through coordination with the TCCC or GCCC, TNCs, Services and Agencies. The Services and Agencies operate and maintain the systems and networks they provide as part of the GIG, in compliance with GIG operations policy and direction of the GNC and appropriate TCCC or GCCC.

The JTF-GNO Service Component Commanders are the Commander, US Army Space and Missile Defense Command (USA SMDC), the US Air Force Commander for USAF NetOps (USAF NetOps / CC), Commander, US Navy Network Warfare Command (USN NETWARCOM) and Commander, US Marine Corps Network Operations and Security Command (MCNOSC). Each of these Service Component Commanders exercises OPCON over their SGNOSC.

The Service Global Network Operations and Security Centers (SGNOSCs) and Computer Emergency / Incident Response Teams (CERT / CIRT) serve as a part of the Service Component to JTF-GNO. The SGNOSC and CERT / CIRT mission is to provide the Service-specific NetOps reporting and SA for the Service's portions of the GIG. The JTF-GNO exercises OPCON of SGNOSCs through its component commands. In response to network events or activities, as determined by CDRUSSTRATCOM or Cdr, JTF-GNO, Service Chiefs or Secretaries shall instantaneously attach Service CERT / CIRT to Commander, JTF-GNO who will exercise Tactical Control (TACON) upon contact with service CERT / CIRT until such time that the responses to the events or activities are declared complete by Cdr, JTF-GNO. In this context, TACON includes the authority for Cdr, JTF-GNO to direct network reconfiguration and defensive actions across the GIG. Cdr, JTF-GNO has the authority to task the Service CERT / CIRT directly, without having to go through the JTF-GNO Component Command.

Defense agencies will follow the NetOps orders and directives issued by USSTRATCOM and JTF-GNO. Service and Agency Systems Management Centers (SMC) and Central Design Authorities (CDA) are in general support of JTF-GNO ensuring that the systems they operate or provide as parts of the GIG are compliant with JTF-GNO guidance.

PERSONNEL: The JTF-GNO is currently authorized more than 250 positions.
Website: http://www.stratcom.mil/ (information only)

Website: www.stratcom.mil/fact_sheets/ (information only)

Last Updated: December 2005

Joint Information Operations Center (JIOC)

Mission: Plans, integrates, and synchronizes information operations in direct support of Joint Force Commanders and serves as the USSTRATCOM lead for enhancing information operations across the Department of Defense.

Tasks:

- Provide continuous and integrated IO planning and execution support to JFCs, including COCOMs, JTFs, JFCCs, the JS, and the OSD. JIOC will provide IO support to national agencies and organizations, allied nations or international organizations as directed.

- Conduct operational analysis which provides the foundation for IO planning within and across geographic regions.

- Assist in the integration of IO into joint exercises.

- Provide IO expertise to assist USSTRATCOM in IO force and capability development.

- Provide EW, PSYOP, MILDEC, and OPSEC expertise to COCOMs through Combatant Command Support Teams (CSTs). JIOC will train and field IO support teams capable of supporting the COCOMs IO staff with integrated IO planning during peacetime operations, contingencies, and exercises. JIOC members will be deployment capable within 72 hours of formal notification.

Capabilities:

- Deployable Combatant Commander support teams – tailored to augment J3 IO Cells

- Reachback – to satisfy Combatant Commander IO requirements with a small forward footprint

- Surge capability – to meet the demands of real world contingencies and exercises

- Visibility across commands – to share lessons learned, and to help synchronize teams regional effects.

- IO simulation and planning tools - IOPCJ, JDSF, ION, RFMP and J-QUAD

Subordination: The Joint Electronic Warfare Center (JEWC) was established by the Secretary of Defense in October 1980 and reported to the Joint Staff. In September 1994, the mission was expanded and the organization was renamed the Joint Command and Control Warfare Center (JC2WC). In 1998, as a result of the Defense Reform Initiative (DRI), the JC2WC was realigned from the Joint Staff to US Atlantic Command. The JC2WC mission was further expanded and resulted in re-designation as the Joint Information Operations Center (JIOC). In October 1999, the JIOC was realigned as a subordinate command of USSPACECOM. On 1 October 2002, the JIOC was realigned as a subordinate command to USSTRATCOM. The Commander, JIOC, reports to the Combatant Commander, USSTRATCOM.

Leadership: The Commander of the JIOC is a nominative position that has always been filled by an USAF General, who is tri-hatted as the Deputy Commander for Information Operations, 8th Air Force and Commander, Air Intelligence Agency.

Personnel: The JIOC is currently authorized 271 positions. Three Allied officers and 100 contractors are fully integrated into the command.

Location: The JIOC is co-located with the Air Intelligence Agency and the Air Force Information Warfare Center (AFIWC) at Lackland AFB, TX.

Website: http://www.jioc.smil.mil

Last updated: December 2005

Service Component Information Operations Organizations

Return to Contents

This Page Intentionally Blank

Return to Contents

Army – 1st Information Operations Command (1st IO Cmd)

Mission: 1st Information Operations Command (Land) deploys IO support teams in order to provide IO planning support and vulnerability assessments in support of military forces and provides an IO reach-back capability to operational and tactical IO staffs as directed. Concurrently, the command conducts continuous Computer Network Defense (CND) operations and CND-Response Actions in coordination with computer network service providers and executes the Threat Analysis (ARAT-TA) program.

Tasks:

1. Organize, train, equip and deploy IO Support Teams to provide IO planning, targeting and execution support and vulnerability assessments as directed.

2. Provide IO "reach-back" support to include; intelligence, planning, and analysis support to deployed Field Support Teams and operational and tactical IO staffs as directed.

3. Provide IO Training Support to LCCs, Army commands, other Service commands, Joint Forces, Agencies, and Activities in support of CAC and as directed by DA G3.

4. Execute the Army Reprogramming Analysis Team-Threat Analysis (ARAT-TA) program.

5. Develop and promote IO interoperability with Joint Forces, other Services, Inter-agencies and Allies as appropriate and as directed.

6. Provide IO support for the assessment of force readiness and capabilities of land component forces to accomplish their assigned missions as directed.

7. As directed, Plan, coordinate and integrate Army Computer Network Operations (CNO), Special Information Operations (SIO), and Special Purpose Electronic Attack (SPEA) capabilities in support of Combatant Commands and land forces on behalf of the Army to accomplish their assigned missions.

8. Conduct continuous Computer Network Defense (CND) operations and CND-Response Actions in coordination with computer network service providers.

9. Establish and maintain the Army's Operations Security (OPSEC) Support Element.

10. Act as the Functional Proponent for Military Deception.

11. Coordinate with and assist TRADOC/CAC in the development and integration of Army IO DOTMLPF requirements, including the development, evaluation, and implementation of IO systems and TTP in combat operations, exercises, and tests and experiments.

1st IO Cmd personnel deploy worldwide, exporting their expertise to commanders through multifaceted Field Support Teams, Vulnerability Assessment Red and Blue Teams, subject matter experts in advanced systems, and all-source databases as well as provide the Army's OPSEC Support Element. Additionally 1st IO Cmd assists in the defense of Army networks, by conducting continuous Computer Network Defense (CND) operations and CND-Response Actions in coordination with computer network service providers. These skilled professionals offer commanders nontraditional options for today's technologically advanced battlespace.

Subordination: 1st IO Cmd is assigned to the U.S. Army Intelligence and Security Command (INSCOM). 1st IO Cmd receives operational taskings from the Army G-3 (Director of Operations, Readiness and Mobilization).

Leadership: The Commander of 1st IO Cmd is an Army Colonel (O-6) from the Military Intelligence branch.

Location: The 1st IO Cmd is located at Ft. Belvoir, VA within the INSCOM HQs building.

https://www.1stiocmd.army.mil/io_portal/Public/Pages/Public_Main.cfm

Last Updated: January 2006.

Return to Contents

Air Force - Air Intelligence Agency

The Air Intelligence Agency (AIA), headquartered at Lackland Air Force Base, Texas, was activated 1 October 1993, and was realigned 1 February 2001 under Air Combat Command (ACC) as a primary subordinate unit. AIA serves as its primary information operations force provider normalizing and synchronizing IO capabilities into the warfighter's arsenal.

Mission

The agency's mission is to deliver multi-source intelligence products, applications, services, and resources. It also provides IO forces and expertise in the areas of information warfare, command and control warfare, security, acquisition, foreign weapons systems and technology, and treaty monitoring, to support Air Force major commands, Air Force components, and joint and national decision makers. With the realignment under Air Combat Command, the AIA commander serves as the Eighth Air Force deputy commander for information operations. The Eighth Air Force with its bomber and IO capabilities is the Air Force's first operational force designed to achieve and maintain information superiority.

Personnel: The agency's 12,000 people serve at approximately 70 locations worldwide.

Organization

The National Air and Space Intelligence Center and Air Force Information Warfare Center are aligned under AIA. The agency is also responsible for mission management and support of signals intelligence operations for the 67th Information Operations Wing, 70th Intelligence Wing, 55th Wing and the 480th Intelligence Wing, all four of which are subordinate to Eighth Air Force. Mission support includes organizing, training and equipping the cryptologic elements of all four wings.

o **National Air and Space Intelligence Center:** The National Air and Space Intelligence Center, with headquarters at Wright-Patterson AFB, Ohio, is the primary Department of Defense producer of foreign aerospace intelligence. NASIC develops its products by analyzing all available data on foreign aerospace forces and weapons systems to determine performance characteristics, capabilities, vulnerabilities, and intentions. Center assessments are also an important factor in shaping national security and defense policies. As the DoD experts on foreign aerospace system capabilities, the center historically has also been involved in supporting American weapons treaty negotiations and verification. Since the start of its organizational lineage in 1961, the center's mission and resources have expanded to meet the challenge of worldwide technological developments and the accompanying national need for aerospace intelligence. In recent years, the emphasis has increasingly shifted toward evaluation of worldwide aerospace systems and the production of tailored, customer-specific products.

o **Air Force Information Warfare Center:** The Air Force Information Warfare Center, with headquarters at Lackland AFB, Texas, is engaged in a myriad of activities supporting its role as the Air Force's information warfare executive agent. It integrates information warfare tactics, training and technology for combatant commanders. The center is comprised of over 900 military and civilian members trained in the areas of operations, engineering, operations research, intelligence, radar technology and communications and computer applications. AFIWC activated Sept. 10, 1993 by combining the Air Force Electronic Warfare Center with elements of the Air Force Cryptologic Support Center's securities directorate and portions of Air Force Intelligence Command. The merger of these organizations provided a solid baseline for the emerging IW mission.

o **67th Information Operations Wing**: The 67th Information Operations Wing, with headquarters also Lackland AFB, manages the agency's global mission. The 67 IOW manages the planning of all-source intelligence. It assists Air Force components in the development of concepts, exercises and employment of AIA forces to support contingency, low-intensity conflict, counter-drug and special operations. Subordinate to the wing are five information operations groups located in the continental U.S., and in the Pacific and European theaters. The wing was activated on Oct. 1, 1993.

o **70th Intelligence Wing**: The 70th Intelligence Wing, with headquarters at Fort Meade, Md., gains and exploits information as a major component of Eighth Air Force's global information operations mission. It provides national decision makers, tactical theater commanders, and warfighters of all services with tailored, timely and actionable information - anywhere, anytime. The wing plans and directs the integration of its components into theater and local exercises, ensuring wartime capabilities are tested and validated, and it assists component commanders with refining their requirements for products and services. Subordinate to the wing are three intelligence groups located in the continental U.S. and in the Pacific and European theaters. The wing was activated on Aug. 16, 2000.

o **55th Wing**: The 55th Wing, with headquarters at Offutt AFB, Neb., conducts worldwide reconnaissance; command, control and communications; Presidential support and international treaty verification as directed by the President, Secretary of Defense, Joint Chiefs of Staff, theater combatant commanders, commanders of major Air Force commands and national intelligence agencies.

o **480th Intelligence Wing**: The 480th Intelligence Wing, with headquarters at Langley AFB, Va., produces and provides timely, tailored intelligence data and capabilities to meet Air Force needs. As a dynamic, worldwide force multiplier, it delivers valuable information to combatants. The wing conducts intelligence, surveillance and reconnaissance tasking processing, exploitation and dissemination processing in support of national interests. It also performs imagery intelligence, cryptologic and measurement and signatures intelligence activities, as well as targeting and general intelligence production, intelligence data handling system network operations, and data/product dissemination. Subordinate to the wing are three intelligence groups located in the continental U.S. The wing was activated Dec. 1, 2003.

Point of Contact

Air Intelligence Agency, Public Affairs Office; 102 Hall Blvd, Ste 234; San Antonio, TX 78243-7036; DSN 969-2166 or (210) 972-2166.

Web site: http://aia.lackland.af.mil/aia/

Last Updated: December 2005.

Return to Contents

Air Force - Air Force Information Warfare Center (AFIWC)

AFIWC is collocated with HQ Air Intelligence Agency at Lackland Air Force Base in San Antonio, Texas. AFIWC is an information superiority center of excellence dedicated to offensive and defensive counter-information and information operations. AFIWC originally activated as the 6901st Special Communication Center in July 1953, and became the Air Force Electronic Warfare Center in 1975. Air Force successes in exploiting enemy information systems during Operation Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare. In response, the AFIWC activated Sept. 10, 1993, combining technical skill sets from the former AFEWC with the Air Force Cryptologic Support Center's Securities Directorate and intelligence capabilities from the former Air Force Intelligence Command.

AFIWC's team of more than 900 military and civilian members are skilled in the areas of operations, engineering, operations research, intelligence, radar technology, communications and computer applications. The members provide information warfare capabilities to the warfighting U.S. Air Force major commands.

Mission: AFIWC is the Air Force's center of excellence for information warfare. AFIWC is responsible for creating the information warfare advantage for combatant forces through exploring, developing, applying and transitioning counter-information technology, strategy, tactics and data to control the information battlespace.

Areas of Expertise

Technology Exploration Demonstration: AFIWC conducts plans and development of Air Force IW programs to satisfy validated warfighter requirements. The center delivers information warfare capabilities such as the Automated Security Incident Measurement System and the Common Intrusion Detection Director System from a suite of more than 90 technology projects. These programs quickly turn around concepts that provide information warfare capability to Air Force units.

Computer & Telecommunication Protection Tools: The Automated Security Incident Measurement System detects and identifies intrusive activities against United States Air Force computer networks. In place at more than 100 Air Force locations, the ASIMs feeds network information to the Air Force Computer Emergency Response Team, also at Lackland Air Force Base, Texas, which assesses Air Force information protection status and takes appropriate actions to protect United States Air Force computer networks and operations. AFIWC executes a comprehensive program to protect U.S. Air Force telecommunication switch systems and services. An important component of this program is a capability to monitor transmissions in order to identify unauthorized dial-up modems, suspect telephone call patterns and other unusual activities. This program will complement ASIMs by protecting installation telecommunication infrastructures.

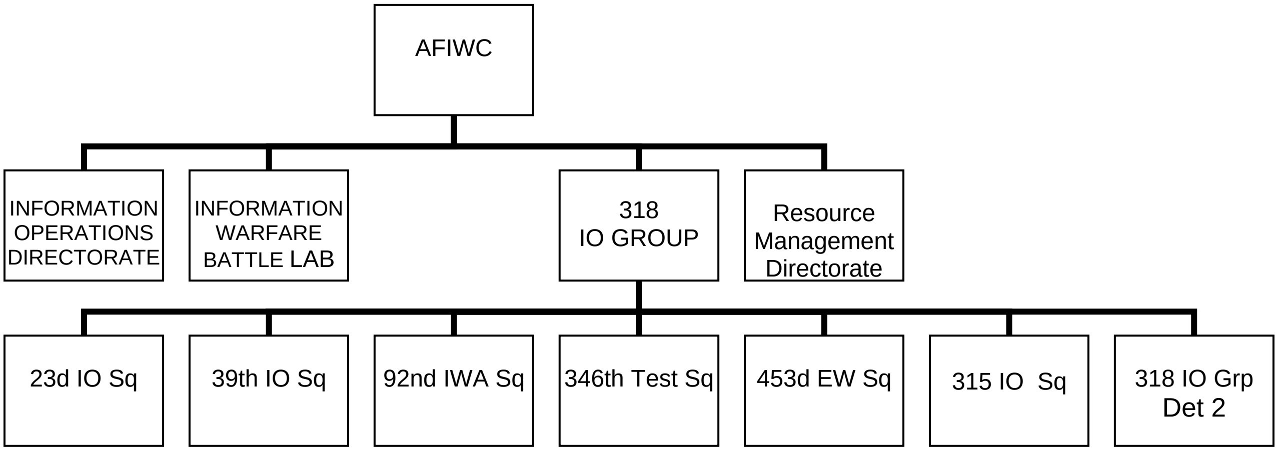
Threat Analysis & Adversary Profiling: AFIWC analyzes threats to various USAF operations and networked systems. The center documents these threats for customers across the Department of Defense to identify U.S. vulnerabilities and maintain threat awareness. AFIWC conceived a computer threat incident database, currently populated with more than 13,000 entries, adopted for use throughout DOD. AFIWC also developed a computer threat analysis tool allowing for profile development of hackers whether operating individually or as part of a larger effort. AFIWC is a producer of the DOD's Modernized Integrated Database and the Command and Control Warfare Operational Support Database which provide combat forces with crucial information on adversary military command, control, and communications. AFIWC conducts integrated analysis studies on designated adversaries providing planners with military options beyond the traditional methods of warfare.

IW Tactics, Techniques & Procedures: AFIWC provides "how to" guidance for Air Force warfighters to ensure proper employment of information warfare capabilities. These tactics, techniques and procedures enable information warriors to plan and execute information warfare as part of an overall aerospace campaign.

Force Training & Assessment: AFIWC is responsible for training Air Force information operations warriors. In that capacity the center maintains a federal library; serves as registrar and manager of AFIWC University and develops cooperative research and development agreements with industry and academia. Through courses such as the Information Operations Integration Course, AFIWC teaches Air Force members how to integrate information warfare as part of traditional air power employment, thus enhancing combat power. AFIWC is also the focal point for Air Force military deception and counter-deception training and is the executive agent for Air Force operations security training. AFIWC conducts adversary information warfare operation and vulnerability assessments, such as red team assessments, by employing realistic threat capabilities and tactics. AFIWC instruction ensures a well-trained core of information warfare experts exists while red team assessments hone the Air Force's information warfare defensive posture.

Modeling & Analysis: The center provides quantitative analysis through modeling and simulation of information warfare activities in Air Force operations. Tailored analytical products are developed in three primary areas: information warfare modeling and simulation, studies of operational systems and support to information warfare acquisition programs.

ORGANIZATION:


AFIWC
INFORMATION OPERATIONS DIRECTORATE
INFORMATION WARFARE BATTLE LAB
318 IO GROUP
Resource Management Directorate
23d IO Sq
39th IO Sq
92nd IWA Sq
346th Test Sq
453d EW Sq
315 IO Sq
318 IO Grp Det 2

Information Operations Directorate: Analyzes US and adversary information operations vulnerabilities, explores leading-edge technologies, prototypes solutions, develops concepts and data applications, and migrates information superiority capabilities to the warfighter. The Information Operations Directorate provides the foundation for Center operations.

Resource Management Directorate: Conducts AFIWC plans and develops Air Force IO programs to satisfy warfighter requirements. It provides planning, programming, and budgeting system actions for AFIWC-executed IO programs. In addition, the directorate manages commander programs to include contracting, deployment, exercise, facility, finance, manpower, security, supply, training, vehicle control, and war plans. It also supplies, operates, and maintains operational communications-computer, test, and special use systems.

Air Force Information Warfare Battlelab, Lackland AFB, Texas: AFIWB's mission is to rapidly identify innovative and superior material or non-material ways to plan and employ information operations capabilities, to organize and train forces for information operations, and to influence IO doctrine and tactics in order to meet current and emerging missions. The Battlelab accomplishes this by conducting operational demonstrations of IO initiatives, evaluating their military worth, and passing the most promising concepts to transition partners to be fielded for operational use. These demonstrations are initiated from concept proposals submitted by individuals and organizations within the military, academia, and industry. All submissions are evaluated for their operational value, technical risk, breadth of application, time for completion, and match to requirements.

318th Information Operations Group Lackland AFB, Texas: Comprised of six unique squadrons and a detachment: the 23d, 39th and 315th Information Operations Squadrons, the 92d Information Warfare Aggressor Squadron, the 346th Test Squadron, the 453d Electronic Warfare Squadron, and 318 IOG, Detachment 2. Air Force lead for delivering Total Force IO capabilities. Seamlessly integrates IO into air/space operations. Tests IO capabilities and develops tactics, techniques and procedures. Conducts full spectrum IO aggressor/Red Team and network/systems vulnerability assessments. Provides electronic warfare analysis and data support. Integrates IO into USAF and joint exercises. Trains and supports warfighters for IO.

23rd Information Operations Squadron Lackland AFB, Texas: Provides tactics training, green teaming, and black cell support to worldwide Air Force and Joint level exercises. Provide advanced IO tactics training throughout DOD through the NOSC Tactician course.

39th Information Operations Squadron Hurlburt Field, Florida: Trains and educates Air Force personnel in the art and science of planning, executing, and assessing Air Force and joint information operations; and maintains technically and operationally proficient instructors to provide classroom instruction, mobile training teams, and advanced distributed learning technologies at Hurlburt Field, Florida and Air Force locations world wide.

92nd Information Warfare Aggressor Squadron Lackland AFB, Texas: Executes full spectrum IO aggressor activities against AF and joint forces through the replication of adversary capabilities and tactics. Conducts IO-focused "Red Team" vulnerability assessments against DoD installations, networks and critical systems. Identifies, reports and recommends solutions to known/found vulnerabilities. Integrates IO aggressor activities into AF and joint exercises to train warfighters.

315th Information Operations Squadron. Advance Air Force information operations capabilities in collaboration with U.S. Government agencies in the National Capital Region and develop Air Force network warfare capabilities and leaders.

346th Test Squadron, Lackland AFB, Texas: Air Combat Command's (ACC) principal IO test unit. Tests, evaluates and assesses operational and emerging IO capabilities for operational forces, national agencies, the acquisition community and DoD customers. Provides USAF's only emissions security testing of critical command and control systems. Maintains ACC's operational ranges for IO test and training exercises. Integrates with the DoD test community.

453rd Electronic Warfare Squadron Lackland AFB, Texas: Develops, maintains, and deploys electronic warfare capabilities to Air Force, Army, Navy and other DoD customers as well as to Coalition partners, in direct support of campaign planning, operations, acquisition and testing. Provides responsive, realistic training simulations and conducts EW capability and vulnerability analyses. Provides threat change analysis, parametric data and is a major contributor to the DoD Electronic Warfare Reprogramming process.

318 Information Operations Group, Detachment 2: USAF lead for integrating information operations (IO) into the Combat Air Forces' training at the operational and tactical levels. Ensures IO integration into the Combined Air Operations Center-Nellis (CAOC-N), the USAF Weapons School and Flag exercises to train air, space and IO professionals. Advances operational test and evaluation of IO weapon systems and develops, tests and documents IO tactics, techniques and procedures.

Web Site: https://afiwcmil.lackland.af.mil/home/index.cfm

Last Updated: December 2005

Return to Contents

Eighth Air Force

Mission:

Headquartered at Barksdale Air Force Base, LA, Eighth Air Force is one of three active-duty numbered air forces (NAF) in Air Combat Command (ACC). It serves as the only information operations and bomber warfighting headquarters.

Organization

Under Air Combat Command (ACC) since 1992, Eighth Air Force controls assets throughout the United States and overseas locations. Eighth Air Force was reorganized into a general purpose numbered Air Force with a warfighting mission to support the U.S. Joint Forces and U.S. Strategic Commands.

In 2001, Headquarters Air Intelligence Agency realigned under ACC as a primary subordinate unit. The agency's two wings, the 67th Information Operations Wing (Lackland AFB, TX) and the 70th Intelligence Wing (Fort Mead, MD), realigned under Eighth Air Force. The move also brought information operations capabilities into a structure similar to those of other Air Force weapons systems provided to commanders. The IO capabilities are integrated with all the other Eighth Air Force warfighting assets.

The Eighth received four additional operational wings as the Air Force moved into the second step of integrating Information Operations into its combat forces in 2002. Eighth Air Force assigned units provide bomber forces, tactical air, electronic warfare, manned and unmanned aerial reconnaissance, intelligence, Airborne Warning and Control System (AWACS) aircraft, Joint Surveillance, Target and Attack Radar System (J-STARS) aircraft, and other capabilities.

The Air Force Network Operations and Security Center (AFNOSC), under Eighth Air Force, began operations in April 2004 and provides around-the-clock centralized command and control of U.S. Air Force-wide networks. This is a mission to control legacy and new information technologies. This center enables the Air Force to maintain its information superiority by providing a single organization to execute both service-specific and joint component responsibilities.

This reorganization takes place as the Air Force continues to blend high-tech information systems with high-tech combat capability. Recent operations have shown that new precision-guided munitions continue to improve the accuracy of Eighth Air Force bombers, and that of unmanned Aerial Vehicles, Airborne Warning and Control System aircraft, and Joint Surveillance, Target and Attack Radar System aircraft are shortening the gap between identifying and targeting enemy forces.

Web Site: www.barksdale.af.mil/8af

Last Updated: December 2005

This Page Intentionally Blank

Return to Contents

Navy - Naval Net Warfare Command (NETWARCOM)

NETWARCOM's establishment shows the Navy's recognition that networks, as warfare enablers, are becoming increasingly important to today's warfighter. NETWARCOM assumed the title of Naval Space Command and serves as the Navy's component to the Commander, United States Strategic Command (USSTRATCOM). NETWARCOM reports administratively to Commander, United States Fleet Forces Command (CFFC) and supports all Fleet Commanders in Chief.

Mission: To act as the Navy's central operational authority for space, information technology requirements, network and information operations in support of naval forces afloat and ashore; to operate a secure and interoperable naval network that will enable effects-based operations and innovation; to coordinate and assess the Navy operational requirements for and use of network/command and control/information technology/information operations and space; to serve as the operational forces' advocate in the development and fielding of information technology, information operations and space and to perform such other functions and tasks as may be directed by higher authority. To serve as the Navy's Functional Component Commander to U.S. Strategic Command.

Purpose: NETWARCOM will be the central operational authority responsible for coordinating all information technology, information operations, and space requirements and operations within the Navy. Establishment of NETWARCOM will better align the various staffs needed to support the concept of one naval network and to support that network's end-to-end operational management.

Subordinate Commands:

- Naval Network and Space Operations Command (NNSOC) in Dahlgren, VA

- Navy IO Command Norfolk, in Norfolk, VA

- Navy Computer Incident Response Team (NAVCIRT) in Norfolk, VA

- Navy IO Command Suitland (formerly Naval Information Warfare Activity – NIWA) in Suitland Virginia

- Navy-Marine Corps Spectrum Center in Dahlgren, VA

- The Commander, Naval Security Group Command (COMNAVSECGRU) has been disestablished as a command. The remaining staff at FT George Meade, MD now serves as the Information Operations Directorate (IOD) part of the NETWARCOM staff.

- As discussed earlier, all of the former Naval Security Group Activities (NSGAs) and detachments have been resubordinated to NETWARCOM and renamed as Navy IO Commands and Navy IO Commands as shown below:

- NAVIOCOM Bahrain
- NAVIOCOM Denver Co
- NAVIOCOM FT George G Meade MD
- NAVIOCOM FT Gordon GA
- NAVIOCOM Hawaii
- NAVIOCOM Medina TX
- NAVIOCOM Menwith Hill UK
- NAVIOCOM Misawa JA
- NAVIOCOM Pensacola FL
- NAVIOCOM Sugar Grove WV
- NAVIOCOM Yokosuka JA
- NAVIODET Washington DC
- NAVIODET Griesheim GE
- NAVIODET Alice Springs NT AS
- NAVIODET Kaneohe Bay HI
- NAVIODET Groton CT
- NAVIODET Brunswick ME
- NAVIODET Digby UK
- NAVIODET Yakima WA
- NAVIODET Seoul KOR
- NAVIODET San Antonio TX
- NAVIODET Chesapeake VA
- NAVIODET Molesworth UK
- NAVIODET Anchorage AK
- NAVIODET Camp H M Smith HI
- NAVIODET Norfolk VA
- NAVIODET Damneck VA

- NETWARCOM is establishing Fleet IO Commands in four locations that will be focused on direct support/tactical planning and execution support for Navy strike groups. The FIOCs will be established as shown below:
  - FIOC Hawaii
  - FIOC Georgia
  - FIOC Texas
  - FIOC Washington

Responsibilities:

The command is responsible for the following sub areas under its specific mission requirements:

- Information Operations
  - Computer Network Offense And Defense
  - Electronic Warfare
  - Operational Security
  - Military Deception
  - Psychological Operations
- Information Technology
  - Network operations
  - Long haul communications
  - IT 21
  - Sea Power 21/FORCENET
  - Network Defense In Depth
  - Bandwidth Utilization
- Naval Space Mission
  - Advocacy of Fleet/Marine Space Requirements
  - Command and Control of Assigned Space Systems
  - UHF SATCOM Operational Management
  - Development of Future Space Applications, Tools, and Professionals
- Personnel
  - Sponsorship and Advocacy for Information Operations Career Force, Information Professional Community, Information Technology/Electronics Technology Ratings, and the Space Cadre.
  - Drive IT/IO/Space Training and Education
  - Help Make Improvements with the Naval Personnel Development Command

Location: Naval Network Warfare Command, 2465 Guadalcanal Road, Norfolk, VA 23521-3228

Web Site: http://www.netwarcom.navy.mil/

Last Updated: December 2005

Navy Information Operations Command Norfolk (NAVIOCOM NORFOLK)

Mission: NIOC Norfolk was established on 04 November 2005 upon the merger of the Fleet Information Warfare Center (FIWC) and the last Naval Security Group Activity (NSGA Norfolk). As its predecessor (FIWC), NIOC Norfolk remains the Navy's Warfare Center of Excellence (WCOE) for Information Operations (IO), with the overall mission of enabling Naval Information Operations (IO) capabilities through tactically focused training, operational planning support to Naval commanders, tactics development, and formulation of IO requirements including research and development priorities.

Responsibilities:

- Acts as the IO academic Center of Excellence responsible for coordination and standardization of operationally focused Naval IO training afloat and ashore.
- Supports Navy component commanders and joint task forces for incorporation of IO capabilities, to include non-kinetic strike, in OPLAN/CONPLAN development and execution, and emerging operations and exercises, as directed by NETWARCOM.
- Acts as NETWARCOM's advocate for IO requirements, recommendations and priorities for research and development, procurement and training in support of IO, including Special Information Operations (SIO) capabilities.
- Acts as Naval Warfare Development Command's primary agent for development of Naval IO doctrine and tactics, techniques, and procedures.
- Acts as the principal agent to NETWARCOM for identification and development of innovative IO technologies and capabilities to support future effects based warfare with non-kinetic options in support of the "Sea Trial" concept.
- Serves as the Navy functional data manager for IO.

Subordination: NIOC Norfolk is a shore activity in an active (fully operational) status under the administrative control of Commander, Naval Network Warfare Command (NETWARCOM).

Subordinate Commands:
Navy IO Command San Diego (formerly FIWC detachment San Diego and NSGA San Diego)
Navy IO Command Whidbey Island (formerly NSGA Whidbey Island)

Leadership: The Commander of NIOC Norfolk is a USN Captain (O6).

Location: 2555 Amphibious Drive, Norfolk, VA 23521-3225
Also: NIOC San Diego,
2024 Trident Way, San Diego Ca 92155-5598; and NIOC Whidbey Island, 1280 West Intruder Street, Oak Harbor, WA 98278-9500.

Contact: http://www.nioc-norfolk.navy.mil/
POC for updating this information: William Malone william.d.malone@navy.mil.

Updated: December 2005.

This Page Intentionally Blank

Return to Contents

Navy Information Operations Command Suitland

Mission: NIOC Suitland is the Navy's principal technical agent and interface to the service and national level agencies engaged in the pursuit of IO technologies and capabilities. . NIOC Suitland's mission includes technical partnership activities with national level agencies for technology development, evaluation and assessment of new IO technologies.

Responsibilities:

- Reinvention Laboratory for IO systems
- RDT&E for Naval IO
- Naval IO modeling and simulation
- Expertise in IO countermeasures
-

Subordination: NIOC Suitland is a shore activity in an active (fully operational) status under the administrative control of Commander, Naval Network Warfare Command (NETWARCOM).

Leadership: The Commander of NIOC Suitland is a USN Captain (O6).

Location:

Updated: December 2005.

This Page Intentionally Blank

Return to Contents

Information Operations Conditions (INFOCONs)

1. **Introduction.** The United States Department of Defense Information Operations Condition (INFOCON) system is a commander's alert system that establishes a uniform process for posturing and defending against malicious activity targeted against U.S. DoD information systems and networks. The INFOCON system was developed for U.S. DoD information systems and networks. However, it is acknowledged that U.S. involvement in future conflicts will likely be within a Combined operations environment. This implies that the success of the Warfighting operations will depend greatly on the ability of the U.S. and allied/coalition partners to ensure continued availability and access to critical mission and support information systems and information networks.

2. **Description.** The INFOCON system is a commander's alert system, characterized by five progressive levels of threats to information networks, and a series of increasing defensive measures that apply to information systems and, to a lesser extent, users of these systems. Specific features assist the commander in using the INFOCON system. A risk mitigation tool aids the commander in proactively declaring postures and directing defensive actions based on advanced indications and warning of hostile activity. The INFOCON system also guides the commander in identifying the INFOCON posture in the event predictive intelligence is not possible. The uniform application of defensive measures promote predictable responses to crises and provide timely, accurate, and clear direction to commanders. Flexibility is built into the INFOCON system to allow additional specific actions to be mandated, based on the threat. Thus, the INFOCON system provides a range of defensive measures that support operations at all levels of conflict, peacetime operations through combat operations, and back to restoration of peace. The INFOCON system pertains to all information systems and networks, including interconnections between public and coalition networks.

3. **Posture Levels.**

The INFOCON system is characterized by five defense postures designed to mitigate risk. These five levels are defined as:

- **NORMAL** (normal activity) Routine CND operations and normal readiness of information systems and networks. Information networks are operational. Normal does not mean an absence of network events, incidents, and intrusions.

- **ALPHA** (increased risk of attack) A condition of preparatory CND operations with a limited risk to operations. This is characterized by an increased intelligence watch and strengthened security measures of information systems and networks.

- **BRAVO** (specific risk of attack) A further increase in CND readiness. Risk to mission accomplishment is moderate, requiring focused network defense and vigilance to maintain network security.

- **CHARLIE** (limited attack) A further increase in CND readiness but less than the maximum CND force readiness. Characterized by concentrated CND operations capable of functioning in a prolonged threat environment.

- **DELTA** (general attack) Maximum CND readiness. Characterized by critical CND operations in which total information assurance resources of the declaring commander are deployed.

Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

4. Authority. The INFOCON system is established by the Secretary of Defense (SecDef), and administered through the Director for Operations, Joint Staff (J-3). The INFOCON system will be administered through the Commander, Joint Task Force for Global Network Operations (JTF-GNO). All combatant commands, Services, directors of Defense and combat support agencies will develop supplemental INFOCON procedures as required, specific to their command and in consonance with this guidance. Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services). Existing policy and procedures on communications security (COMSEC) may be integrated into local INFOCON procedures at the commander's discretion.

5. Applicability. This document provides guidance for standardized procedures and sets responsibilities for authorizing and communicating INFOCONs as part of information operations (IO) throughout the Department of Defense. The information contained herein applies to the Joint Staff; Services; combatant commands; Defense agencies; and joint, combined, and other DoD activities throughout the entire conflict spectrum -- peacetime through war.

6. Assumptions. Several critical assumptions were made about the nature of computer network attack (CNA) in developing the DoD INFOCON system. Understanding these assumptions is essential to effectively implement this system.

a. Shared Risk. In today's network-centric environment, risk assumed by one is risk shared by all. Unlike most other military operations, a successful network intrusion in one area of responsibility (AOR) may, in many cases, facilitate access into other AORs. This necessitates a common understanding of the situation and responses associated with the declared DoD INFOCON. These actions must be carried out concurrently in all AORs for an effective defense.

b. Advance Preparation. Preparation is key, given the speed and reduced signature of CNA. Protective measures must be planned, prepared, exercised, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack. Prevention of system compromise is preferable, but may not be achievable.

c. Anonymity of Attacker. Attributing the attack to its ultimate source, if possible, will normally not occur until after the attack has been executed. This limits the range and type of options available to military decision-makers. To effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

d. Characterization of the Attack. Distinguishing between hacks, attacks, system anomalies, and operator error may be difficult. The most prudent approach is to assume malicious intent until an event is assessed otherwise.

7. **Structure.** This paragraph explains the INFOCON structure, including level, brief description, criteria to declare, and recommended actions. The criteria listed are broad guidance for the commander to consider when declaring an INFOCON, not concrete thresholds. All criteria for a particular INFOCON need not be met to change to that level.

LABEL **(DESCRIPTION)**	**CRITERIA**	**RECOMMENDED ACTIONS**
NORMAL **Normal Activity**	No significant activity.	• Ensure all mission critical information and information systems (including applications and databases) and their operational importance are identified. • Ensure all points of access and their operational necessity are identified. • On a continuing basis, conduct normal security practices. For example: • Conduct education and training for users, administrators, and management. • Ensure an effective password management program is in place. • Conduct periodic internal security reviews and external vulnerability assessments. • Conduct normal auditing, review, and file back-up procedures. • Confirm the existence of newly identified vulnerabilities and install patches. • Employ normal reporting procedures IAW para 8d. • Periodically review and test higher level INFOCON actions.
ALPHA **Increased Risk of Attack**	Indications and warning (I&W) indicate general threat. Regional events occurring which affect U.S. interests and involve potential adversaries with suspected or known CNA capability. Military operation, contingency or exercise planned or ongoing requiring increased security of information systems. Information system probes, scans or other activities indicating a pattern of surveillance.	• Accomplish all actions required at INFOCON normal. • Execute appropriate security practices. For example: • Increase level of auditing, review, and critical file backup procedures. • Conduct internal security review on all critical systems. • Heighten awareness of all information system users and administrators. • Execute appropriate defensive tactics. • Employ normal reporting procedures IAW para 8d. • Review and test higher level INFOCON actions, and consider proactive execution.
BRAVO **Specific Risk of Attack**	I&W indicate targeting of specific system, location, unit or operation. Major military operation or contingency, planned or ongoing. Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance. Network penetration or denial of service attempted with no impact to DoD operations.	• Accomplish all actions required at INFOCON ALPHA. • Execute appropriate security practices. For example: • Increase level of auditing, review, and critical file backup procedures. • Conduct immediate internal security review on all critical systems. • Confirm existence of newly identified vulnerabilities and install patches. • Disconnect unclassified dial-up connections not required for current operation. • Execute appropriate defensive tactics. • Ensure increased reporting requirements are met IAW para 8d. • Review and test higher level INFOCON actions, and consider proactive execution.

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
BRAVO **Specific Risk of Attack**	I&W indicate targeting of specific system, location, unit or operation. Major military operation or contingency, planned or ongoing. Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance. Network penetration or denial of service attempted with no impact to DoD operations.	• Accomplish all actions required at INFOCON ALPHA. • Execute appropriate security practices. For example: • Increase level of auditing, review, and critical file backup procedures. • Conduct immediate internal security review on all critical systems. • Confirm existence of newly identified vulnerabilities and install patches. • Disconnect unclassified dial-up connections not required for current operation. • Execute appropriate defensive tactics. • Ensure increased reporting requirements are met IAW para 8d. • Review and test higher level INFOCON actions, and consider proactive execution.
CHARLIE **Limited Attack(s)**	Intelligence attack assessment(s) indicate a limited attack. Information system attack(s) detected with limited impact to DoD operations: Minimal success, successfully counteracted. Little or no data or systems compromised. Unit able to accomplish mission.	• Accomplish all actions req'd at INFOCON BRAVO. • Execute appropriate response actions. For example: • Conduct maximum level of auditing, review and critical file back-up procedures. • Consider MINIMIZE on appropriate computer networks and telecommunications systems (limit traffic to mission essential communication only - See CJCSI 6900.01A) • Reconfigure information systems to minimize access points and increase security. • Reroute mission-critical communications through unaffected systems. • Disconnect non-mission essential-critical networks • Employ alternative modes of communication and disseminate new contact information. • Execute appropriate defensive tactics. • Ensure increased reporting requirements are met IAW para 8d. • Review and test higher level INFOCON actions, and consider proactive execution.
DELTA General Attack(s)	Successful information system attack(s) detected which impact DoD operations. Widespread incidents that undermine ability to function effectively. Significant risk of mission failure.	• Accomplish all actions required at INFOCON CHARLIE. • Ensure increased reporting requirements are met IAW para 8d. • Execute applicable portions of continuity of operations plan (See DODD 3020.26, Continuity of Operations, Policy and Planning). For example: • Designate alternate information systems and disseminate new communication procedures internally and externally. • Execute procedures for ensuring graceful degradation of information systems. • Implement procedures for conducting operations in "stand-alone" mode or manually. • Isolate compromised systems from rest of network. • Execute appropriate defensive tactics.

8. Procedures.

a. Determining the INFOCON. There are three broad categories of factors that influence the INFOCON: operational, technical, and intelligence, including foreign intelligence and law enforcement intelligence information. Some factors may fall into more than one category. The INFOCON level is based on significant changes in one or more of them. Appendix C describes several factors that may be considered when determining the INFOCON. DoD organizations are frequently confronted with unauthorized access to information systems. The decision to change the INFOCON should be tempered by the overall operational and security context at that time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may only warrant INFOCON ALPHA or NORMAL during peacetime, but may warrant INFOCON CHARLIE during a crisis; or it may warrant a high INFOCON at the affected unit, but not throughout the command or the Department of Defense as a whole.

b. Declaring INFOCONs. The Joint Staff J3/Commander, JTF-GNO (Cdr, JTF) will recommend changes in DoD INFOCON through the CJCS to the SecDef IAW paragraph 3. Assimilation and evaluation of information to assess the CND situation DOD-wide will be a collaborative effort focused at the Joint Staff/JTF-GNO. The Secretary of Defense may delegate declaration authority to the J-3/Cdr, JTF. Commanders are responsible for assessing the situation and establishing the proper INFOCON based on evaluation of all relevant factors. Commanders may change the INFOCON of their organizations; however, they must remain at least as high as the current INFOCON directed by SecDef or the Chairman of the Joint Chiefs of Staff. The commander will report changes in INFOCON IAW subparagraph 7d.

c. Response Measures. Response measures associated with INFOCONs are normally recommended actions unless specifically directed by SecDef. Ideally, CND operations will be based on advanced warning of an attack. The intelligence community is developing a capability to provide warning which will become of increasing value as it matures. Measures should be commensurate with the risk, the adversary's assessed capability and intent, and mission requirements. Over-aggressive countermeasures may result in self-inflicted degradation of system performance and communication ability, which may contribute to the adversary's objectives. Commanders must also consider the impact imposing a higher INFOCON for their command will have on connectivity with computer networks and systems of other commands. Combatant commands will notify the Joint Staff if recommended or directed response measures conflict with theater priorities. Additionally, response measures directed by combatant commands will take precedence over response measures directed by Service INFOCONs when applicable. Regardless of the INFOCON level declared at the affected site, it is incumbent upon the affected site to report all unauthorized accesses in a timely manner IAW subparagraph 7d.

d. Reporting. Technical reporting will be accomplished IAW CJCSI 6510.01b, "Defensive Information Operations Implementation." Report violations of the law (such as unauthorized access to military computer networks and systems) to servicing military counterintelligence organizations IAW DODI 5240.6, "Counterintelligence Awareness and Briefing Program," and with local and Service/command policy. However, INFOCONs assess potential and/or actual impact to DoD operations and must be reported through operational channels. Additional guidance on INFOCON reporting follows.

(1) Reporting Channels. Combatant commands, Services, and DoD agencies will report INFOCON changes and summary reports to the Joint Staff through the National Military Command Center (NMCC): CJCS NMCC WASHINGTON DC//J3/DDIO//. Combatant commands, Services, and DoD agencies will designate a reporting authority and establish reporting procedures for organizational entities under their jurisdictions. Service entities under the operational control of a combatant command will follow the reporting instructions of that combatant command. Individual Service policy may require information copies to higher Service headquarters. Those entities not reporting directly to a CINC will follow Service-reporting procedures (usually to the Service operations center, which would then forward the information

to the NMCC).

(2) Reporting Frequency. Services, combatant commands, and Defense agencies will report INFOCON changes to the NMCC NLT 4 hours after the INFOCON has changed. Provide whatever information is available at the time and indicate fields that are unknown or unavailable. Report information missing from the initial report in a follow-up report when it becomes available. Services, combatant commands, and Defense agencies may dictate more frequent internal reporting to subordinate components.

(3) Report Formats. Reports of changes in INFOCON should be accompanied by an operational assessment of the situation when appropriate. Reports will include, as a minimum:

(a) For all INFOCONs: unit/organization and location, date/time of report, current INFOCON, reason for declaration of this INFOCON, response actions taken, POC (name, rank, duty title, contact information).

(b) INFOCON BRAVO and higher. All of the above, plus: unit/organization mission, current operation(s) (name, type, and AOR) unit is supporting, upcoming operation(s) (name, type, AOR, and dates) unit is projected to support, Service computer emergency/incident response team (CERT/CIRT) or JTF-GNO NetDefense incident number and law enforcement agency (LEA) case number with POC contact information.

(c) INFOCON CHARLIE and higher. All of the above, plus: system(s) affected (network, classification, application, database/data file), degree to which operational functions are affected (command and control; intelligence, surveillance and reconnaissance; movement/maneuver; sustainment; fires; and protection), impact (actual and/or potential) on current/planned missions and/or general capabilities, restoration priorities, workarounds.

(4) Dissemination of DoD INFOCON. The Joint Staff/JTF-GNO will send notification to combatant commands, Services, and agencies when the DoD INFOCON is changed. Commands, Services, and agencies are responsible for notifying units assigned to them. Notification will include the following information:

(a) Date/time of report.

(b) Current INFOCON.

(c) Reason for declaration of this INFOCON.

(d) Current/planned operation(s) or capabilities, units/organizations, networks, systems, applications or data assessed to be impacted or at risk.

(e) Recommended or SecDef-directed actions.

(f) References to relevant technical advisories, intelligence assessments, etc.

(g) POC contact information.

9. Security. Classification guidance and disclosure policy concerning IO is addressed in DoDI 3600.2, “Classification Guidance for Information Operations.” Specific guidance related to INFOCON follows.

a. INFOCON labels and descriptions are unclassified.

b. Generic defensive measures, when not tied to a specific INFOCON, are unclassified. Specific measures may be published in a classified appendix, if required.

c. Measures to be taken by all personnel, regardless of INFOCON, are unclassified.

d. General criteria to declare an INFOCON are FOR OFFICIAL USE ONLY (FOUO). Specific criteria may be published in a classified appendix, if required.

e. Classification of the measures associated with a particular INFOCON is the responsibility of the originator and will be classified according to content. However, the measures associated with a particular INFOCON, in aggregate, may require a higher classification than the individual measures. The measures associated with a particular INFOCON, in aggregate, will be FOUO at a minimum.

f. The operational impact of a successful information attack is classified SECRET or higher.

g. CNA intelligence assessments are classified SECRET or higher.

h. Information associated with an ongoing criminal investigation of a CNA may be considered law-enforcement sensitive.

i. A combatant command, Service, or agency may authorize release of its INFOCON system and procedures to allies or coalition partners as necessary to ensure effective protection of its information systems. Locally developed INFOCON procedures should use DoDI 3600.2 and the guidance above when considering release to allies or coalition partners.

j. Changes in INFOCON are operational security (OPSEC) indicators and must be protected accordingly. The criteria and response measures are also of value to foreign intelligence Services in assessing the effectiveness of a CNA and in analyzing DoD's response. Do not post INFOCON procedures in publicly accessible locations such as unit web pages on unclassified networks and bulletin boards accessible to outsiders.

10. Relationship of INFOCON to Other Alert Systems. The INFOCON, THREATCON, DEFCON, CNA-WATCHCON, and conventional WATCHCON all interact with each other when the situation warrants it. The INFOCON may be changed based on the world situation (THREATCON, DEFCON), the intelligence community's level of concern (CNA-WATCHCON, conventional WATCHCON), or other factors . Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

a. The defense condition (DEFCON) is a uniform system of progressive conditions describing the types of actions required to bring a command's readiness to the level required by the situation.

b. The threat condition (THREATCON) is a process that sets the level for a terrorist threat condition at a given location, based on existing intelligence and other information.

c. A watch condition (WATCHCON) is part of the defense warning system indicating the degree of intelligence concern with a particular warning problem.

d. A CNA-WATCHCON is an intelligence assessment that takes into account CNA threat levels, as well as the overall political situation (reference CJCSM 3402.01A, "Alert System of the Chairman of the Joint Chiefs of Staff").

e. The INFOCON addresses risk of attack and protective measures for information and information systems.

Last Updated: December 2005

This Page Intentionally Blank

Return to Contents

Glossary

NOTE: Definitions which are proposed in the current draft version of Joint Publication 3-13, *Information Operations*, are also used here and appear in italics.

Area of influence - A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (JP 1-02)

Area of interest - That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. See also area of influence. (JP 1-02)

Civil affairs (CA) - The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral or hostile area of operations in order to facilitate military operations and consolidate operational objectives. CA may include performance by military forces of activities and functional normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. (JP 1-02)

Civil military operations (CMO) - Group of planned activities in support of military operations that enhance the relationship between military forces and civilian authorities and population and which promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups. (JP 3-57)

Combat Camera (COMCAM) - Visual information documentation covering air, sea, and ground actions of the Armed Forces of the United States in combat or combat support operations and in related peacetime training activities such as exercises, war games, and operations. (JP 1-02)

Command and control (C2) - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP1- 02)

Command and control system - The facilities, equipment, communications, procedures, and personnel essential for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)

Command and control warfare (C2W) - The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command and control; electronic warfare; information operations; intelligence; military deception; operations security; psychological operations . (JP 1-02)

Computer network attack (CNA) - The operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-51)

Computer network defense (CND) - Defensive measures taken to protect and defend information, computers, and networks from disruption, denial, degradation or destruction. (JP 3-51)

Computer Network Exploitation (CNE) - *Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (Draft JP 3-13)*

Computer Network Operations (CNO) - *Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (Draft JP 3-13)*

Computer security (COMPUSEC) - The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)

Counterdeception - Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 1-02)

Counterintelligence - The information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Counterpropaganda – (Army) Programs of products and actions designed to nullify propaganda or mitigate its effects. (FM 3-13)

Cyber counterintelligence *- Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligences service collection efforts that use traditional methods to gauge cyber capabilities and intentions. (Draft JP 3-13)*

Cyberspace - The notional environment in which digitized information is communicated over computer networks. (JP 1-02)

Deception action - A collection of related deception events that form a major component of a deception operation. (JP 1-02)

Deception concept - The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the combatant commander's strategic concept. (JP 1-02)

Deception course of action - A deception scheme developed during the estimate process in sufficient detail to permit decision-making. At a minimum, a deception course of action will identify the deception objective, the deception target, the desired perception, the deception story, and tentative deception means. (JP 1-02)

Deception event - A deception means executed at a specific time and location in support of a deception operation. (JP 1-02)

Deception means - Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. physical means Activities and resources used to convey or deny selected information to a foreign power. (Examples include military operations, including exercises, reconnaissance, training activities, and movement of forces; the use of dummy equipment and devices; tactics; bases, logistic actions, stockpiles, and repair activity; and test and evaluation activities.) b. technical means Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power through the deliberate radiation, re-radiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles. c. administrative means Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02)

Deception objective - The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (JP 1-02)

Deception story - A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (JP 1-02)

Deception target - The adversary decision maker with the authority to make the decision that will achieve the deception objective. (JP 1-02)

Defensive information operations - The integration and coordination of policies and procedures, operations, personnel, technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purpose. (JP 1-02)

Desired perceptions - In military deception, what the deception target must believe for it to make the decision that will achieve the deception objectives. (JP 1-02)

Disinformation - (Army) Disinformation is information disseminated primarily by intelligence organizations or other covert agencies designed to distort information, or deceive or influence US decision makers, US forces, coalition allies, key actors or individuals via indirect or unconventional means. (FM 3-13)

DoDD - Department of Defense Directive.

Electromagnetic spectrum - The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)

Electromagnetic pulse (EMP) - The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 1-02)

Electronics security - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non communications electromagnetic radiation, e.g., radar (JP 1-02)

Electronic warfare (EW) - Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy; it includes the three major subdivisions of electronic attack (EA), electronic protection (EP), and electronic warfare support (ES); EA is the use of either electromagnetic or directed energy to attack personnel, facilities, or equipment with intent of degrading, neutralizing, or destroying enemy combat capability; EP is the protection of friendly combat capabilities against the undesired effects of friendly or enemy use of EW; ES involves actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition (JP 3-13)

Global Information Grid (GIG) - The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid (GIG) includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense (DOD), National Security, and related intelligence community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. (JP 1-02)

Global information infrastructure - The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. (JP 1-02)

High-payoff target - A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through war-gaming, that must be acquired and successfully attacked for the success of the friendly commander’s mission. (JP 1-02)

High-value target - A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander’s area of interest. (JP 1-02)

Human factors *- The psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization (Draft JP 3-13)*

Influence operations- (Air Force) Employment of capabilities to affect behaviors, protect operations, communicate commander’s intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander’s objectives (AFDD 2-5)

Information - (1) The meaning assigned to sensing from the environment. (2) On the cognitive hierarchy, consist of processed data that provides further meaning with further transformation. Processing activities include filtering, formatting, organizing, collating, correlating, plotting, translating, categorizing, and arranging among others. (JP 1-02)

Information assurance (IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP1-02)

Information environment *- The aggregate of individuals, organizations or systems that collect, process, or disseminate information; also included is the information itself (Draft JP 3-13)*

Information management (IM) - (Army) The provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision making. It uses procedures and information systems to collect, process, store, display, and disseminate information. (FM 3-13)

Information operations (IO) - The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own. (DoDD 3600.1/JP 3-13)

Information operations cell - (Army definition, but also functionally described within JP 3-13) A grouping of staff officers to plan, prepare and execute information operations formed around the information operations section. The output of the IO cell is input to the targeting cell. (FM 3-13)

IO Capability Specialist - A functional expert in one or more of the IO core capabilities (see IO Career Force, below next). They serve primarily in their specialty areas but may also serve as IO planners after receiving IO planner training. (DoDD 3608.11)

IO Career Force - The military professionals that perform and integrate the core IO capabilities of EW, CNO, PSYOP, MILDEC, and OPSEC. The IO Career Force consists of IO Capability Specialists and IO Planners. (DoDD 3608.11)

IO Planner - A functional expert trained and qualified to execute full spectrum IO. They usually serve one or more tours as an IO capability specialist prior to assignment as an IO planner and may hold non-IO positions throughout their careers. (DoDD 3608.11)

INFOCON - Information Operations Condition

Information security (INFOSEC) - The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. (JP 1-02)

Information superiority - The degree of dominance in the information environment which permits the conduct of operations without effective opposition. (JP 1-02)

Information systems (INFOSYS) - The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Information - 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Interagency coordination - Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies, nongovernmental organizations, and regional and international organizations for the purpose of accomplishing an objective. (JP 1-02)

Joint intelligence preparation of the battlespace (JIPB) - The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the total battlespace environment; describing the battlespace's effects; evaluating the adversary; and determining and describing adversary potential courses of action. The process is used to analyze the air, land, sea, space, electromagnetic, cyberspace, and human dimensions of the environment and to determine an opponent's capabilities to operate in each. Joint intelligence preparation of the battlespace products are used by the joint force and component command staffs in preparing their estimates and are also applied during the analysis and selection of friendly courses of action. (JP 1-02)

Joint restricted frequency list (JRFL) - A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. (JP 1-02)

Joint targeting coordination board (JTCB) - A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and refining the joint integrated prioritized target list. The board is normally comprised of representatives from the joint force staff, all components and, if required, component subordinate units. (JP 1-02)

Measures of effectiveness (MOE) - Tools used to measure results achieved in the overall mission and execution of assigned tasks. Measures of effectiveness are a prerequisite to the performance of combat assessment. Also called MOEs. See also combat assessment; mission. (JP 1-02)

Military Deception (MILDEC) - Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02)

Military operations other than war - Operations that encompass the use of military capabilities across the range of (MOOTW) military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. (JP 1-02)

Military support to public diplomacy*- Those activities and measures taken by the DOD components to support and facilitate public diplomacy. (Draft JP 3-13.)*

Nongovernmental organization (NGO) - Transnational organizations of private citizens that maintain a consultative status with the Economic and Social Council of the United Nations. Nongovernmental organizations may be professional associations, foundations, multinational businesses, or simply groups with a common interest in humanitarian assistance activities (development and relief). (JP 1-02)

Operational security (OPSEC) - The process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems; (b) determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation; also called OPSEC (JP 1-02)

Perception management - (Army) Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. (FM 3-13)

Physical destruction - (Army) The application of combat power to destroy or neutralize adversary forces and installations. It includes direct and indirect forces from ground, sea, and air forces. Also included are direct actions by special operations forces. (FM 3-13)

Physical security - That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft (JP1-02)

Priority national intelligence objectives - A guide for the coordination of intelligence collection and production in response to requirements relating to the formulation and execution of national security policy. They are compiled annually by the Washington Intelligence Community and flow directly from the intelligence mission as set forth by the National Security Council. They are specific enough to provide a basis for planning the allocation of collection and research resources, but not so specific as to constitute in themselves research and collection requirements.(JP 1-02)

Propaganda - Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. See also black propaganda; grey propaganda; white propaganda. (JP 1-02)

Psychological operations (PSYOP) - Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives; also called PSYOP (JP1-02)

Psychological operations assessment team (POAT) - A small, tailored team (approximately 4 - 12 personnel) that consists of psychological operations planners and product distribution/ dissemination and logistic specialists. The team is deployed to theater at the request of the combatant commander to assess the situation, develop psychological operations objectives, and recommend the appropriate level of support to accomplish the mission. (JP 1-02)

Psychological operations impact indicators - An observable event or a discernible subjectively determined behavioral change that represents an effect of a psychological operations activity on the intended foreign target audience at a particular point in time. It is measured evidence, ascertained during the analytical phase of the psychological operations development process, to evaluate the degree to which the psychological operations objective is achieved. (JP 1-02)

Psychological operations support element - A tailored element that can provide limited psychological operations support. Psychological operations support elements do not contain organic command and control capability; therefore, command relationships must be clearly defined. The size, composition and capability of the psychological operations support element are determined by the requirements of the supported commander. A psychological operations support element is not designed to provide full-spectrum psychological operations capability; reachback is critical for its mission success. (JP 1-02)

Public affairs (PA) - Those public information, command information, and community relations activities directed toward both the external and internal public with interest in the DOD. (JP 1-02)

Public diplomacy (PD) - Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. (JP 1-02)

Public information - Information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or nonobjectionable to the responsible releasing agency. (JP 1-02)

Reachback - The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)

Spectrum management - Planning, coordinating, and managing operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (JP 1-02)

Strategic communication *- The transmission of integrated and coordinated United States Government themes and messages that advance United States interests and policies through a synchronized interagency effort that includes public diplomacy, public affairs, and information operations, in concert with other political, economic, and military actions (Draft JP 3-13)*

Target audience (TA) *- An individual or group selected for influence or attack by means of psychological operations. (Draft JP 3-13.)*

The DoD Dictionary of Military and Associated Terms is available on line at:

www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

Last updated : January 2006